# Serv-U® File Server User's Manual

# Table of Contents

# Notices

This document is provided for use with the setup and maintenance of the Serv-U File Server. This manual is provided "AS IS" and without warranties as to the accuracy of the information or any other warranties whether expressed or implied. Because of the various hardware and software environments into which Serv-U ® may be put, NO WARRANTY OF FITNESS FOR A PARTICULAR PURPOSE IS OFFERED.

Good data processing practice dictates that any new program should be thoroughly tested by the user with non-critical data before relying on it. The user must assume the entire risk of using the program. ANY LIABILITY OF THE SELLER WILL BE LIMITED EXCLUSIVELY TO PRODUCT REPLACEMENT OR, AT THE SELLER'S DISCRETION, A REFUND OF PURCHASE PRICE.

Contact Information

Rhino Software, Inc.
P.O. Box 53
Helenville, WI 53137
U.S.A.

Phone: +1 (262) 560-9627
Fax: +1 (262) 560-9628

Office Hours: 9 AM – 5 PM Central Time, United States

Sales Support: http://www.RhinoSoft.com/Sales

Technical Support: http://www.RhinoSoft.com/Support

Knowledge Base: http://www.RhinoSoft.com/KB

Corporate Website: http://www.RhinoSoft.com/

# How To Purchase Serv-U

Serv-U is available as a fully functional Gold Edition trial for 30 days after the date of initial installation. In order to continue using Serv-U with its full set of features, a Serv-U license must be purchased.

A license can be purchased online at http://www.Serv-U.com/purchase/. Simply choose which Edition of the Serv-U File Server is required and the quantity to purchase (discount pricing applies for bulk purchasing). A Serv-U File Server license must be purchased before adding an FTP Voyager JV license to your shopping cart. Licenses of FTP Voyager (our premier FTP client software) may also be bundled at the time of purchase at a substantial discount.

Pricing information can be found at: http://www.Serv-U.com/pricing/.

If you have lost your registration ID, it can be retrieved at: RhinoSoft.com Online Customer Service Center.

Once the purchase has been completed, an email containing the registration details is immediately sent. If it is not received within an hour, check your Spam filter to make sure that the email has not been filtered. Occasionally, the .reg installation file attached to our messages is blocked. If this should happen, simply register using the "Register Manually" directions in the email.

Purchase orders can be sent to RhinoSoft.com in one of three ways:

1. E-Mail PO to a Sales Representative at: http://www.Serv-U.com/sales/.
   *(PDF/JPG/GIF Format Preferred)*
2. Fax PO to +1 (262) 560-9628
3. Mail directly to RhinoSoft at the following address:

   RhinoSoft.com
   P.O. Box 53
   Helenville, WI 53137
   U.S.A.

# Serv-U Editions

Serv-U File Server is available in three different editions.

## Serv-U Bronze

Serv-U Bronze is an entry-level server with low user limits and only two interfaces for transferring files:

- FTP and basic web transfer interface (via HTTP)
- One domain with twenty-five concurrent connections
- 50 user accounts
- Virtual path mapping
- Transfer ratios and quotas

## Serv-U Silver

Serv-U Silver extends the capabilities of Serv-U Bronze by adding:

- Encrypted FTPS (SSL/TLS) transfer interface
- Three domains with 100 concurrent connections
- 250 user accounts
- User password recovery

## Serv-U Gold

Serv-U Gold is our most popular edition. It removes all user and domain limits, adds two more secure protocols and provides the ability to integrate into enterprise technology.

- Encrypted SFTP (SSH) transfer interface
- Encrypted web transfer interface (via HTTPS)
- Remote web-based administration
- Unlimited domains with an unlimited number of concurrent connections
- Unlimited number of user accounts
- FIPS 140-2 support, certified through OpenSSL (Certificate #1051)
- Custom HTTP Logo
- User and Group Statistics
- ODBC database storage of user and group accounts
- NT-SAM / Active Directory based user accounts
- Event-based automation: run programs, send email and show balloon tips

# System Requirements

## Supported Platforms

Serv-U is supported exclusively on the following versions of Windows:

- Windows XP SP2+
- Windows Vista
- Windows 7
- Windows Server 2003
- Windows Server 2008

Both **32-bit** and **64-bit** (x64) builds of Windows are supported.

## Suggested Hardware

The minimum hardware requirements for Serv-U are:

1 GHz+ Pentium / AMD CPU
256 MB RAM
70 MB Disk Space
800x600 VGA Video Card & Monitor
Internet Explorer 6+

## Recommended Hardware

3 GHz+ Pentium / AMD CPU
1 GB RAM
100 MB Disk Space
1024x768 VGA Video Card & Monitor
Internet Explorer 8

NOTE: Serv-U is a multi-threaded application, allowing it to make effective use of resources to provide a fast user experience for any number of users – in particular, heavy downloading/uploading since these operations run in their own threads. However, it is not necessary to have these higher hardware specs to run Serv-U effectively.

# Getting Started

1) Download Serv-U from http://www.Serv-U.com/dn.asp. This site will always have the latest release of Serv-U available for download as a trial. The trial can be registered at any time to the full release after your purchase, and does not require any additional configuration.

2) Double click the installation file to start the installation. If you are using Windows Vista, Windows 7 or Windows Server 2008 you must have administrator privileges to start the installation process. You may need to confirm a Windows User Account Control dialog to indicate you did initiate the installation process.

3) Serv-U supports installation in English, German, French, Italian, Japanese, Russian, and Simplified/Traditional Chinese. Select your preferred language then click "OK". NOTE: At this point you are selecting only the default language for the Management console. Users connecting remotely can select any language they wish when they connect to Serv-U, from the supported languages.

4) Follow the simple installation process. The options to select from include: the Serv-U installation folder, the name of the folder to be created in the Start Menu, and whether or not to install Serv-U as a service. Installation as a service is recommended because it allows Serv-U to run even when no users are logged on to the server console.

5) After the installation, click "Finish" to launch the Serv-U Management Console.

# Creating the First Serv-U Domain

Serv-U Domains are collections of users and groups that share common setting, such as transfer rate limitations, service listeners and directory access rules. In most cases, all of your users and settings will exist in the same domain, with no need to create separate domains. Cases for using different domains are discussed in the Virtual Hosts section.

NOTE: This does NOT mean that all users share access to the same files. Each user in Serv-U has unique permissions to the directories that you define, and does not have access to any files or folders unless you explicitly grant them that access.

After first installing Serv-U, no domains will exist. The Serv-U Management Console will prompt you to create an initial Domain. The Domain Wizard will ask you for the following information:

- Domain Name: This is the casual name used in Serv-U to refer to your collection of users. This can be something formal like ftp.mydomain.com or simply "My Domain"
- Description (optional): A text description of the domain and its purpose.
- Listeners: Serv-U supports FTP, HTTP (All Editions), FTP (Silver & Gold Editions) and SFTP with HTTPS (Gold Only). These listeners can be configured during the setup process. If you already have a web server, you may need to set the HTTP/HTTPS listeners to use a nonstandard port like 8080/8081 or disable them by "unchecking" those listeners.
- IP Address (optional): If Serv-U should listen for incoming connections on a single specific IP, enter it here. This must be the IP address assigned to a NIC on the server. In most cases, this should be left blank.
- Password Encryption Mode: If Password Recovery (Silver / Gold Edition Only) is to be used, the "Password Encryption Mode" should be set to "Simple Two-Way" to allow Serv-U to recover passwords for users. There is also the "No Encryption" option, which is not recommended as it is the least secure method of storing user passwords. In most cases, the Server Default is recommended.
- Finished! You can now click "Finish" to start your first Domain. If you wish, follow the Serv-U prompt to create a new user account.

# Creating Your First Serv-U User

Serv-U users are unique accounts with privileges to access a specific set of administrator-defined folders and files. To create user accounts quickly and easily, click the "Wizard" button in the Domain Users menu and follow these steps:

1) Select a unique Login ID for your user account (also called a "username"). If you wish, you can also specify a full name and email address (used in password recovery or E-Mail Events.
2) Enter a password for your user account.
3) Select the Home Directory of the user account, and if desired disable the "Lock user in home directory" option. The default and recommended option is "enabled".
4) Select the user's permissions. The two options are "Read-Only" and "Full Access". Full Access does NOT allow the user to execute files remotely.
5) Click "Finish".

This user can then log on using any of the protocols enabled in the Domain Details | Listeners menu.

# Serv-U Server Concepts

The Serv-U File Server makes use of several concepts that aid in the understanding of how to configure and administer your File Server as a single, hierarchical unit. There are four related levels of configuration to the Serv-U File Server: the Server, the Domain, the Group, and the User. Of all of these, only the Group is optional - all the other levels are mandatory parts of the File Server. An explanation of each level is provided below.

## User Account Types

User accounts can be defined in various ways on the Serv-U File Server, including:

- Domain Users - Defined at the Domain level, Domain Users can only log in to the Domain under which they are created.
- Global Users - Defined at the Server level, Global Users are accounts that can log in to any Domain on the File Server.
- Database Users - Available at both the Server and Domain level, Database Users are stored in an external database accessible through ODBC and supplement the local account database.
- Windows Users - Defined at the Domain level, Windows Users are Windows accounts either on the local system or accessible through a domain controller that supplement the local account database and allows a client to log in to the File Server using their Windows login credentials.

Since User accounts can be assigned at the various levels with the same login ID, a hierarchy is used by Serv-U to determine which account takes precedence. The User account types listed above are listed in the order of precedence. Where User accounts can be specified at both the Domain and Server levels, the Domain level account always takes precedence over the Server one.

When creating Users, consider what kind of access they need, and select the appropriate location for the User account accordingly - time and effort can be saved by entering such settings at the Server level to remove the need for multiple User accounts at the Domain level.

## User Collections

Unlike Groups, User Collections do not offer any level of configuration to the User accounts they contain. Instead, they simply offer a way to organize users into containers for ease of viewing and administration. For example, Collections can be created to organize User accounts based upon Group membership; However, they must be manually maintained when User accounts change Group membership.

## Server

The Server is the basic unit of the Serv-U File Server and the highest level of configuration available. It represents the File Server as a whole and governs the behavior of all Domains, Groups, and Users. The Serv-U File Server ships with a set of default options that can be overridden on a per setting

basis. Thus, the Server is at the top-level of the hierarchy of configuring Serv-U. Domains, Groups, and Users inherit their default settings from the Server. Inherited settings can be overridden at each of these lower levels. However, some settings are exclusive to the Server, such as the PASV port range.

## Domain

A Server can contain one or more Domains. Domains are the interface through which Users connect to your File Server and access a specific User account. A Domain's settings are inherited from the Server. It also defines the collection of settings that all of its Groups and User accounts inherit. If a Server setting is overridden at the Domain level, then all of its Groups and User accounts inherit that value as their default value.

## Group

The Group is an optional level of extra configuration provided to make it easier to manage related User accounts that share many of the same settings. By using a Group, administrators can quickly make changes that propagate to more than one User account instead of having to manually configure each one separately. A Group inherits all of its default settings from the Domain it belongs to. It defines the collection of settings inherited by all Users who are a member of the Group. Virtually every User level setting can be configured at the Group level, or overridden at the User level.

## User

The User is at the bottom of the hierarchy. It can inherit its default settings from multiple Groups (if it's a member of more than one Group) or from its parent Domain (if it's not a member of a Group or the Group doesn't define a default setting). A User account identifies a physical connection to the File Server and defines the access rights and limitations of that connection. Settings overridden at the User level cannot be overridden elsewhere and are always applied to connections authenticated with that User account.

# User Interface Conventions

The Serv-U File Server uses a consistent method of representing configuration options in a manner that not only conveys the current value of the option, but also whether or not that value is the default (or inherited) value. Traditionally, this has been done with something called a tri-state checkbox. The tri-state checkbox has two major drawbacks:

1. The default state does not clearly convey the current value of the option. In some versions of Windows, the box is checked with a gray background - even if the option isn't currently enabled!
2. They can only be used to represent binary values, which is to say they can only represent two values - on or off.

The Serv-U File Server uses a different, easy to understand convention that overcomes these drawbacks. When an option is inheriting its value from a parent, the text of the option is displayed in regular, unbolded text. The value that is displayed (whether it's a text value or a checkbox) can change to reflect changes made to the parent where the item is currently inheriting its value.

However, if the value is overriding the default, the text of the value is displayed in bold. The value that is currently displayed is always the value of that option, regardless of changes to its parent.

## Understanding User Interface Conventions

To better illustrate the user interface conventions, consider the following case file.

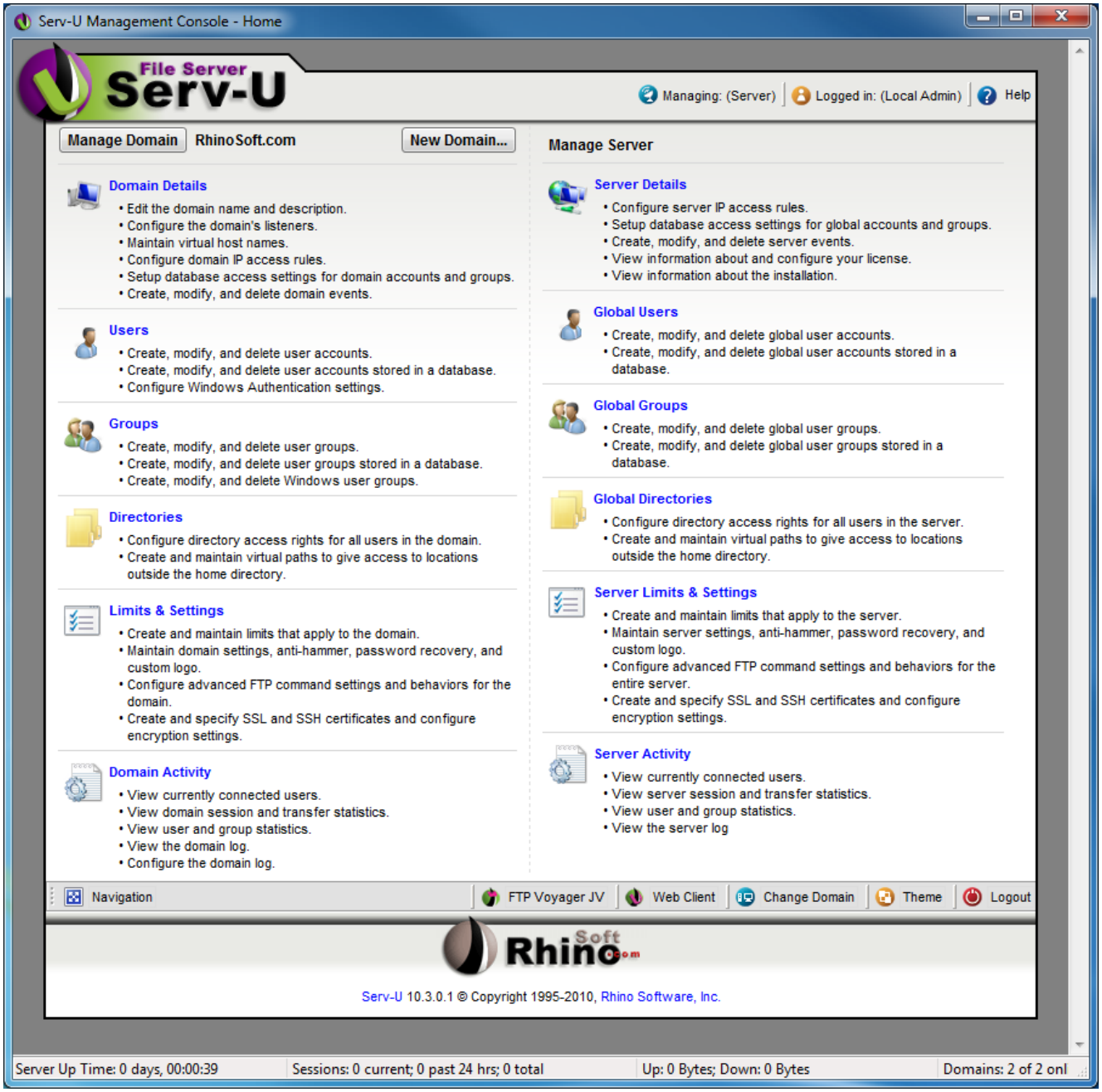
Acme Technology Co. is a computer repair company that maintains a Serv-U File Server providing global access to shared corporate resources to their traveling technicians. Each technician has their own account on the File Server. To facilitate easy administration of the user accounts, the File Server administrator has made each user account a member of the "Technician" group. This group's Administration Privilege is set to No Privilege since none of the technicians have any File Server administration duties.


A technician receives a promotion. In addition to his current technician duties, he is also given administration privileges on the File Server so he can assist other technicians with their accounts. The File Server administrator can simply edit the technician's user account and change the Administration Privilege to Domain Administrator. The text of this option turns bold to reflect that it is overriding the default value (No Privilege) that the user account inherits from its membership to the "Technician" group.

At a later date, the Administration Privilege can be reverted back to the default value inherited from the "Technician" group by selecting the Inherit default value option in the "Administration Privilege" drop-down box.

# The Serv-U Management Console

The Serv-U Management Console is designed to provide quick and easy access to the File Server's configuration options in a familiar way. When viewing a configuration page, you can return to the main Management Console page at any time by clicking on the Serv-U logo in the top-left corner.



## Management Console Layout

The Management Console is presented in the familiar control panel style layout and arranged in to categories of related options. Clicking a category header, such as "Users", displays the user account management screen. From this screen, each of the sub-category configuration options is available. A sub-category can also be selected to go directly to that sub-category's configuration page.

For Server Administrators, the Management Console is displayed in two columns. The right column displays categories related to configuring server-wide options and settings. The left column displays categories related to configuring the active domain. To change the active domain, click the Manage Domain button in the top-left corner of the Management Console and select a different domain to administer. Alternatively, the Change Domain button is available in bottom-right corner of the footer. This method of changing the active domain can be employed from any Management Console page.

Domain Administrators only have access to configuring settings and options for their applicable domain and do not have access to the server-level categories displayed to System Administrators.

## Navigation Menu

The Navigation menu is located in the lower-left corner of the screen and provides direct links to all of the Serv-U configuration categories. It is context sensitive and displays the relevant categories for the selection being configured (Domain or Server) as well as an expandable list of configuration options for the currently selected category.

## Tabbed Configuration Pages

When opening a category from the Management Console, all related sub-category pages are displayed in tabs on the same screen. This allows for quick navigation between related configuration options.

## Launching the Web Client

While configuring the Serv-U File Server, an HTTP session can be launched by clicking the appropriate launch button in the toolbar at the bottom of the page. If licensed for use, the Web Client is available and runs from within the browser. If licensed for use, FTP Voyager JV can also be launched using the Java Runtime Environment, by clicking on the FTP Voyager JV button.

## Changing Themes in Serv-U

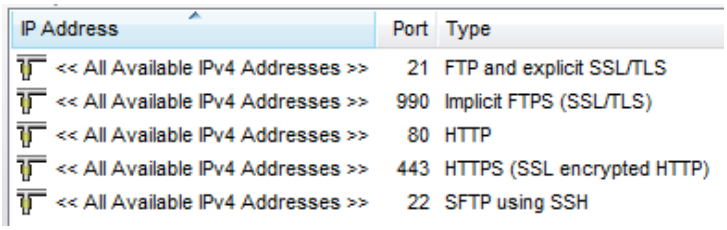
The "Theme" button, used to launch the theme menu, is located in the lower-right corner of the screen. The menu lists the available themes available to change the look and feel of Serv-U. Simply select a theme from the drop down combo box then click the "OK" button. The theme will be loaded without needing to refresh the page.

# Serv-U Network Configuration Primer

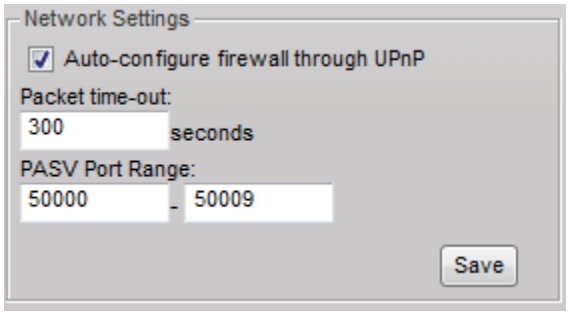
Under ideal circumstances, services and applications like the Serv-U File Server are installed on dedicated servers in a DMZ with their own dedicated IP address. However, with security concerns, existing network configurations and a shortage of available IPv4 addresses many times Serv-U must be installed on a server behind a firewall or router and use "Port Forwarding" to handle FTP traffic. This allows networks with limited public IP addresses to host many services without needing to pay extra for additional public IP addresses or costly and unnecessary network hardware. It is also optimal when integrating with Windows Active Directory, since AD integration requires that the server be a member of Active Directory.

To configure Serv-U to work with your router or firewall, you must first configure the router (and/or firewall) to forward your desired file transfer ports to the internal IP address of your server. While FTP is the most common one used, other protocols are also available in Serv-U. These protols and their ports are typically:

- FTP - FTP port 21 and PASV port range 50000-50009
- FTPS (Implicit) - FTP port 990 and PASV port range 50000-50009
- SFTP - Port 22
- HTTP - Port 80
- HTTPS - Port 443

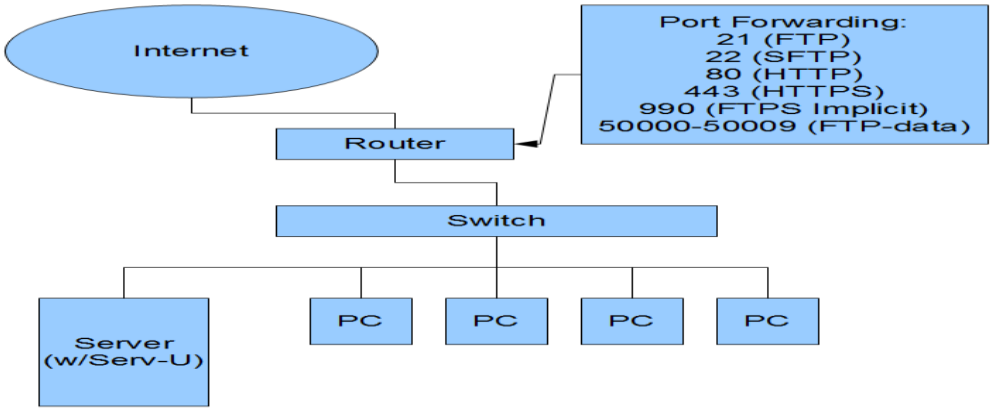



This allows the file transfer traffic to be routed through the router and directly to Serv-U. Routers typically call this option "Port Forwarding", and it is usually found in the "Advanced" options of most residential and simpler commercial routers. When you configure port forwarding, be sure to configure the "PASV Port Range" in the "Server Limits & Settings | Settings" menu to 50000-50009 as well.



To make this process even simpler, Serv-U includes support for a protocol known as "Universal Plug and Play". This allows Serv-U to automatically configure the router or firewall with your settings, eliminating the need to configure any settings yourself. However, in most cases it is better to manually configure the router.

Below is a diagram of Serv-U in a typical small/medium office network.




## PASV IP Address

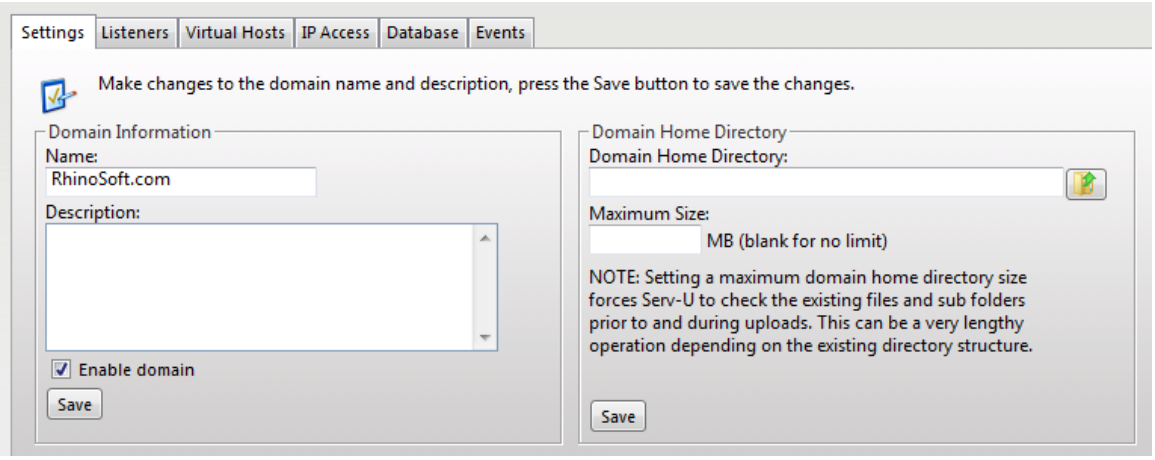
Each "FTP and Explicit SSL/TLS" and "FTPS Implicit" Listener includes a configuration option called "PASV IP Address or Domain Name". This option exists because the FTP and FTPS protocols use two different connections in order to communicate. The first connection is the most well-known, and occurs on port 21 – this is called the Control Channel, and is used for the server and client to communicate about what data will be transferred, what user is logging on, and more. The lesser-known connection is the Data Channel, a second connection on which directory listings and files are transferred. Most clients use Data Channel connections in "PASV mode", which takes place on the port rnage of 50000-50009.

As part of the communication process, Serv-U must be able to tell clients how to connect to the server, including what port number and IP address to use. Since this may be different than the IP address used to establish the initial FTP connection, it is communicated in a special "227" message sent by Serv-U to the client. The IP address that is sent is normally the private IP address of the server, because the server does not know the router's IP address. The router then automatically adjusts the 227 message and adds the correct IP address.

The problem occurs when either the router does not perform this task or the client connects using an encrypted connection, which makes it impossible for the router to read the FTP session and perform this task. In this case, Serv-U relies on the administrator to tell it what information it needs to send to the client. To provide this information, the "PASV IP Address" field in the "Domain Details | Listeners" FTP entries should be updated with the public IP address of the server, or the domain name of the

server. In most cases, the domain name is actually preferable because this way if the IP address changes, the domain name will be updated and therefore Serv-U will be updated without any intervention. For users with dynamic IP addresses who are using dynamic DNS service, this is doubly helpful.

# Domain Name & Description




Each Domain must be uniquely identified with a Domain Name. If a name is provided that is not unique, an error message is shown indicating that a unique name is required for each Domain. The Domain Name is used purely for administrative purposes and is not visible or accessible to Users.

In addition, each Domain can have additional descriptive information associated with it through the Description. Like the Domain Name, the Description text is also only available to users with administrative access. This field is useful for describing the purpose of the domain or summarizing the resources made available by the Domain's existence on the File Server.

Domains can be temporarily disabled by unchecking the Enable domain checkbox. While disabled, the Domain is completely inaccessible to all Users. The Domain still exists on the File Server, all settings are preserved, and it can still be administered while it is disabled. To make the Domain accessible to Users again, check the Enable domain checkbox.

After making changes to any of the above Domain settings, click the Save button to apply the changes.

## Domain Home Directory

System Administrators can limit the disk space available to a Domain by configuring a home directory for the Domain and specifying a maximum size. The Domain's home directory does not affect User directory access rules, nor does it restrict the paths that are available to a User in any way. However, in order to calculate the amount of disk space in use by a Domain, Serv-U must know the root directory under which it expects all Domain files to be stored.

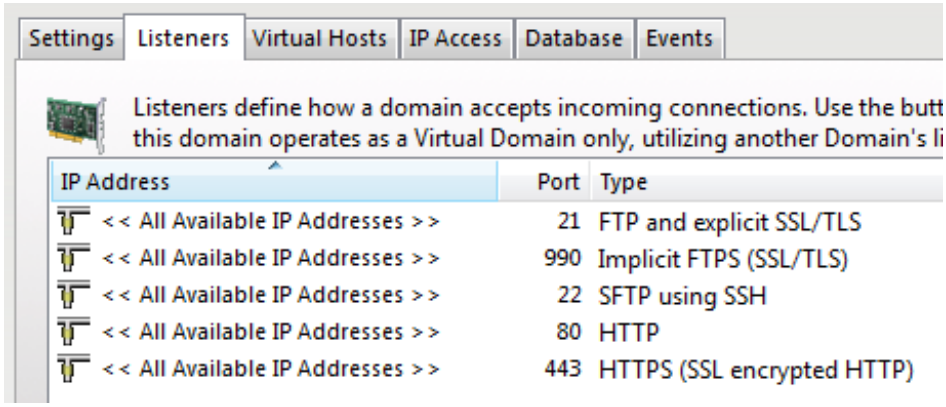
To specify the Domain home directory, enter a path in the field labeled Domain Home Directory. The Browse button can also be used to select a path. When creating a Domain Administrator account for this Domain, it is suggested that their home directory be the same, which ensures that all Users of the Domain are placed in a subdirectory of the Domain's home directory. Enter the amount of disk space,

in megabytes (MB), available to the Domain in the Maximum Size field. Leaving this field blank or entering "0" does not impose a maximum size on the Domain. When a limit is imposed, any upload that would cause this maximum size to be exceeded is rejected by the Server. Click the Save button to apply these changes.

NOTE: Calculating the amount of disk space in use by a Domain can be a time consuming operation depending on the directory structure.

# Domain Listeners

The Serv-U File Server offers a highly configurable interface for enabling the different file sharing protocols on a Domain. Listeners are added, edited, and deleted using the appropriately labeled button. Each Domain can listen on multiple ports and IP addresses by adding a listener bound to the desired IP address and port. In addition to selecting these connection attributes for a listener, a file sharing protocol must also be selected. A listing and short description of the file sharing protocols supported by the Serv-U File Server follows.




## FTP - File Transfer Protocol

FTP is the traditional protocol for transferring files over the Internet. It normally operates on the default port 21. Traditionally, FTP is handled in plain-text, however SSL connections are explicitly supported through the use of the AUTH command.

## FTPS - File Transfer Protocol Using SSL

FTPS is identical to FTP, however connecting to a listener configured for FTPS means that an SSL connection is required before any protocol communication is performed. This is commonly referred to as Implicit FTPS, which normally takes place on the default port 990.

## SFTP - Secure File Transfer Using SSH2

SFTP is a secure method of transferring files through a secure shell session. It performs all protocol communications and data transfers over the same port eliminating the need to open multiple ports in firewalls as is commonly required when using FTP. SFTP sessions are always encrypted. SFTP operates on the default port 22.

## HTTP - Hypertext Transfer Protocol

HTTP is the protocol used to browse Web sites. It's also a simple method for downloading and transferring files. One benefit to adding an HTTP listener to a Domain is the availability of the Web

Client, which allows users to transfer files to and from your File Server without the need for a stand-alone client. HTTP traditionally operates on port 80.

## HTTPS - Hypertext Transfer Protocol using SSL

HTTPS is identical to HTTP except all communications are secured using SSL. Like FTPS, a secure connection is implied when connecting to a listener running the HTTPS protocol. The default port for HTTPS is 443.

# Adding a Listener

After clicking the Add button, the listener configuration dialog is shown. After configuring each of the listener options, click the Save button to add the listener to the Domain.

## Type

Select the desired file sharing protocol that is to be supported by this listener. Each listener can only support a single protocol. To add more file sharing protocols to the Domain, create new listeners for each protocol. A brief description of the support file sharing protocols is found above.

## IP Address

A listener can be bound to a single IP address by entering it here. If the File Server does not have an external IP address, (e.g., it's behind a router), this field can be left blank. Leaving the field blank tells Serv-U to listen on all available IP addresses.

## PASV IP Address or Domain Name (FTP ONLY)

If the listener is supporting the FTP protocol, this additional field is available to specify a separate IP address to use for PASV mode data transfers. Entering an IP address here ensures that PASV mode works properly on both unsecured and secured connections. If the File Server does not have an external IP address, try using a dynamic DNS service and entering your dynamic DNS domain name in this field. Serv-U resolves your dynamic DNS domain name to ensure it always has the proper external IP address for PASV command responses.

## Use only with SSL connections

This option allows the PASV IP Address or domain name to only be used for SSL connections where it is always necessary to provide the PASV IP Address to connecting clients. When this option is enabled, the IP Address specified for PASV mode will not be provided to clients connecting via non-SSL FTP.

## Use with LAN connections

Normally, Serv-U does not use the PASV IP Address for connections coming from the Local Area Network (computers on the same network as Serv-U). When this option is enabled, the PASV IP Address is also used for LAN connections.

## Port

The default port for the selected protocol is automatically provided. However, any port between 1 and 65535 can be used. When using a non-standard port, clients must know the proper port in advance when attempting to connect to the Domain. If using a non-standard port, we recommend using a value above 1024 to prevent potential conflicts.

## Enable listener

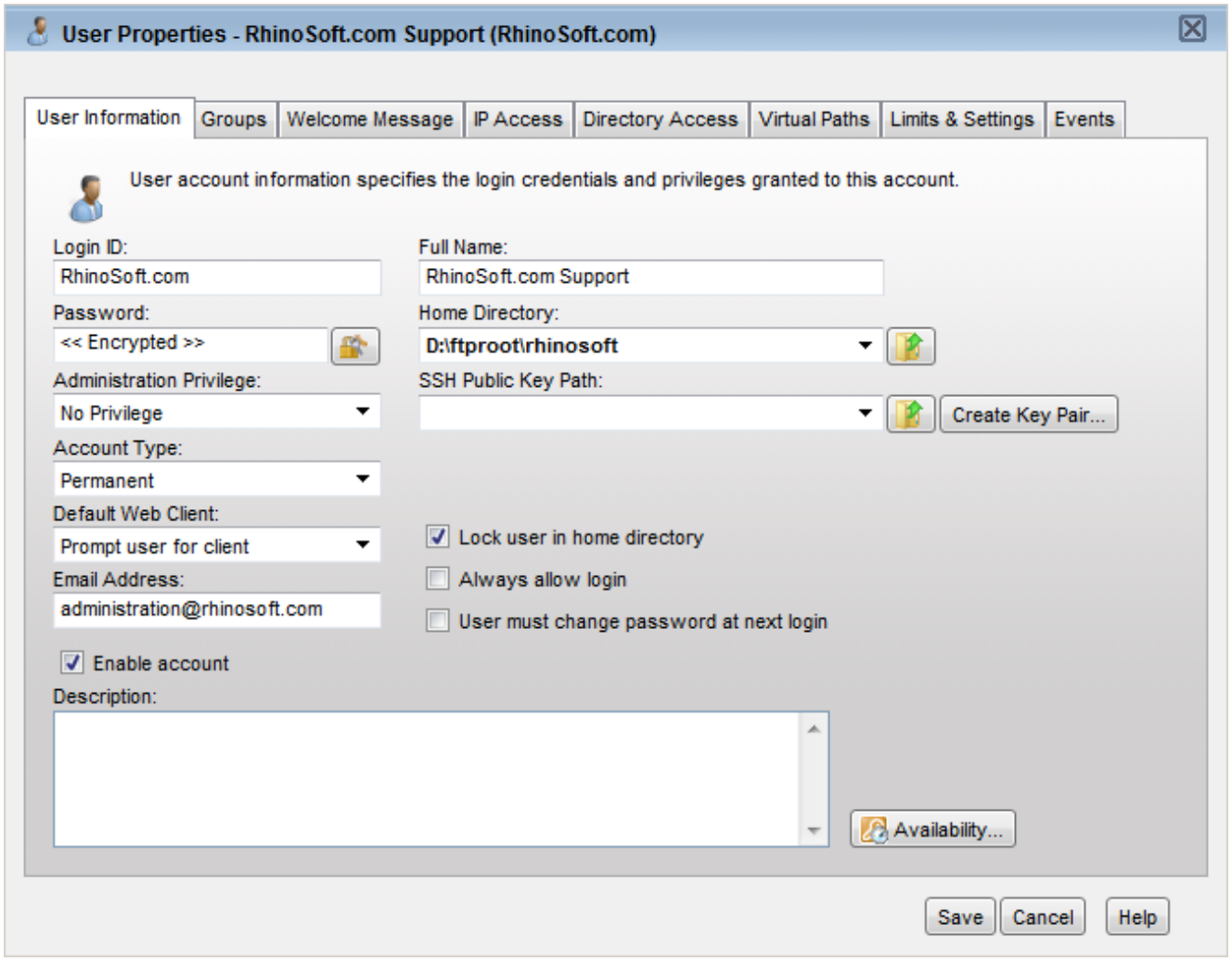
Unchecking this box temporarily disables a listener. While disabled, listeners are displayed with a different icon in the list.

# Pure Virtual Domains

Serv-U supports the ability for multiple Domains to "share" the same listeners. In other words, one Domain can possess the necessary listener configurations while the other Domain "piggybacks" on the first one. In this way, the second Domain exists in a virtual way. To have a Domain "piggyback" on the listener configurations of existing Domains, leave the listener list blank for the Domain. The "piggybacking" Domain needs to have at least one Virtual Host defined for it.

This method of "piggybacking" only works with the FTP and HTTP protocols as they are the only two file sharing protocols that specify a method for identifying the desired host after a connection is established. For FTP connections, the client must issue a HOST command to identify the desired domain. For HTTP connections, the browser automatically handles providing the necessary host header to Serv-U based upon the domain name used to establish the HTTP connection.

# User Information




A User account consists of many attributes and settings. The User Information tab contains general information about the User account including login credentials, the home directory, and the type of account. Detailed information on each of the available attributes is found below.

## Login ID

The login ID is provided by the client as one part of authenticating the session to the File Server. In addition to the login ID, clients must provide a password to complete authentication. Login IDs must be unique for each account specified at that level. Login IDs may not contain any of the following special characters: \ / < > | : ? *.

NOTE: There are two special login IDs: "Anonymous" and "FTP". These login IDs are synonymous with one another and can be used for guests on your File Server. These users do not require a

password, which should be left blank in this case. Instead, Serv-U requires users who log on with one of these accounts to provide their email address to complete the login process.

## Full Name

The full name of the account is available to specify additional identifying information about the account. It is not used by clients when they log in.

## Password

The password is the second item required for a session to be authenticated with the File Server. The password should be kept a secret and not shared with anyone other than the person that owns the account. A strong password contains at least 6 characters including a mix of upper and lowercase letters and at least one number. Restrictions can be placed on the length and complexity of passwords through limits. See the Help documentation on Password Limits for more information.

Additionally, the "Lock" icon next to the "Password" field allows a new random password to be generated for a user. This new password will follow defined password length requirements. By default, all passwords are 8 characters long and are complex. If the "Minimum Password Length" is equal to or less than four characters, the password will be four characters long - otherwise, generated passwords will follow the specified domain value.

## Administration Privilege

A User account can be granted one of three types of administrative privileges: No Privilege, System Administrator, or Domain Administrator. The value of this attribute can be inherited through Group membership.

A User account with No Privilege is a regular user account that can only log in to transfer files to and from the File Server. The Serv-U Management Console is not available to these User accounts.

A System Administrator has the ability to perform any File Server administration activity including creating and deleting Domains, User accounts, or even updating the File Server's license. A User account with System Administrator privileges that is logged in through HTTP remote administration can essentially administer the server as they had physical access to the machine.

A Domain Administrator can only perform administrative duties for the Domain to which their account belongs. A Domain Administrator is also restricted from performing Domain-related activities that may affect other Domains. The Domain-related activities that may not be performed by Domain Administrators consists of configuring their Domain listeners or configuring ODBC database access for the Domain.

A Group Administrator can only add, edit, and remove users who are members of the first Group that the Group Administrator is a member of. This allows the Group Administrator to modify users who are in the same scope – for example, a Group Administrator of the "Accounting" group can add, remove, and edit users who are in the Accounting group but is not able to grant permissions to files outside of the Accounting group, and cannot edit or access users outside of that Group. Group

Administration is designed to be used by department leads and junior administrators with the need to modify certain user accounts, without making changes to the Domain or Server.

Serv-U also supports read-only administrator accounts which can allow administrators to log in and view configuration options at the domain or server level, greatly aiding remote problem diagnosis when working with outside parties. Read-only administrator privileges are identical to their full-access equivalents, except that they cannot change any settings or create/delete/edit user accounts.

NOTE: When configuring a User account with administrative privileges, take care in specifying their home directory. An administrator with a home directory other than "\" (root) that is locked in their home directory may not use file paths outside of their home directory when configuring the File Server.

## Home Directory

The home directory for a User account is where the User is placed immediately after logging in to the File Server. Each User must have a home directory assigned to it, although it can be specified at the Group level if the User is a member of a Group. Home directories must be specified using a full path including the drive letter or UNC share name. If the home directory is not found, Serv-U can be configured to create it.

When specifying the home directory, the %USER% macro can be used to insert the login ID in to the path. This is used mostly to configure a default home directory at the Group level or within the new User template to ensure that all new Users have a unique home directory. When combined with a Directory Access Rule for %HOME%, a new User can be configured with a unique home directory and the proper access rights to that location with a minimal amount of effort.

The %DOMAIN_HOME% macro may also be used to identify the user's home directory. For example, to place a user's home directory into a common location use %DOMAIN_HOME%\%USER%.

The home directory can be specified as "\" (root) in order to grant system-level access to a User, allowing them the ability to access all system drives. In order for this to work properly, the User must not be locked in their home directory.

## SSH Public Key Path

The SSH public key can be used to authenticate a user when logging into the the Serv-U File Server. The public key path should point to the key file in a secured directory on the server. This path can include the following macros:

%HOME% - The Home Directory of the user account
%USER% - The Login ID, used if the public key will have the Login ID as part of the file name
%DOMAIN_HOME% - The Home Directory the Domain, set in Domain Details | Settings, used if the keys will be in a central folder relative to the domain Home Directory

Examples:

%HOME%\SSHpublic.pub
%HOME%\%USER%.pub
%DOMAIN_HOME%\SSHKeys\%USER%.pub

Click here for information on creating a SSH key pair.

## Account Type

By default, all accounts are permanent and exist on the File Server until manually deleted or disabled. An account can be configured to be automatically disabled or even deleted on a specified date by configuring the Account Type. After selecting the appropriate type, the Account Expiration Date control appears. Click on the calendar or expiration date to select when the account should be disabled or deleted.

## Default Web Client

If your Serv-U license enables the use of FTP Voyager JV, then users connecting to the File Server through HTTP can choose which client they want to use after logging in. Instead of asking users which client they want to use, a default client can also be specified. If this option is changed, it overrides the option specified at the Server or Domain level. It can also be inherited by a User through Group membership. Use the Inherit default value option to reset it to the appropriate default value.

## Email Address

Serv-U Events can use the "Email Address" field when sending email notifications to groups, and password recovery using the Web Client requires an email address to send a recovered password to a user. Enter an email address here to allow email notifications or password recovery for the user account.

## Lock user in home directory

A user that is locked in their home directory may not access paths above their home directory. In addition, the actual physical location of their home directory is masked as Serv-U always reports it as "/" (root). The value of this attribute can be inherited through Group membership.

## Enable account

Uncheck this box to disable the current account. Disabled accounts remain on the File Server but cannot be used to log in. To re-enable the account, check the Enable account box again.

## Always Allow Login

Enabling this option means that the User account is always permitted to log in, regardless of restrictions placed upon the File Server such as IP access rules or a maximum number of sessions. It is useful as a fail-safe in order to ensure that critical system administrator accounts can always remotely access the File Server under all conditions. As with any option that allows bypassing

access rules, care should be taken in granting this ability. The value of this attribute can be inherited through Group membership.

## Description

The description allows for the entry of additional notes that are only visible by administrators.

## Availability

This feature limits when users can connect to this server. Limitations may be placed on the time-of-day as well as the day-of-the-week. When logging in outside the specified available times users are presented a message that the user account is currently unavailable.

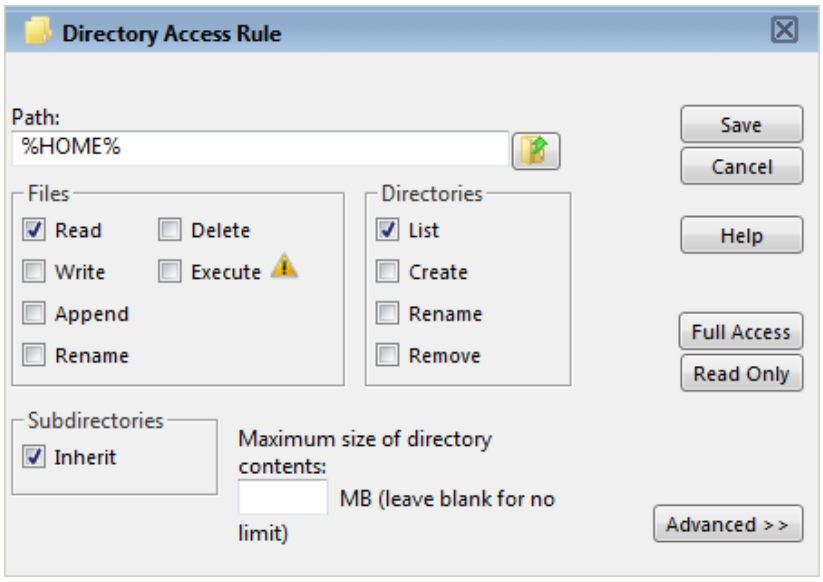
# Directory Access Rules

Directory Access rules define the areas of the system that are accessible to user accounts. While traditionally restricted to the User and Group levels, Serv-U extends the usage of Directory Access rules to both the Domain and Server levels through the creation of global Directory Access rules. Directory Access rules specified at the Server level are inherited by all Users of the File Server. When specified at the Domain level, they are only inherited by Users belonging to that Domain. The traditional rules of inheritance apply where rules specified at a lower level (e.g., the User level), override conflicting or duplicates rules specified at a higher level (e.g., the Server level).

When setting the Directory Access path, the %USER%, %HOME%, %USER_FULL_NAME%, and %DOMAIN_HOME% variables are available to simplify the process. For example, use %HOME%/ftproot/ to create a Directory Access rule that specifies the "ftproot" folder in the user's home directory. Directory access rules specified in this manner are "portable" in the event that the actual home directory changes while maintaining the same subdirectory structure. This leads to less maintenance for the File Server administrator. If the %USER% variable is specified in the path, it is replaced with the user's login ID. This variable is useful in specifying a Group's home directory to ensure that Users inherit a logical and unique home directory. The %USER_FULL_NAM% variable can be used to insert the "Full Name" value into the path (the user must have a "Full Name" specified for this to function). For example, the user "Tom Smith" could use D:\ftproot\%USER_FULL_NAME% for "D:\ftproot\Tom Smith". Finally, the %DOMAIN_HOME% macro may also be used to identify the user's home directory. For example, to place a users and their home directory into a common directory use %DOMAIN_HOME%\%USER%.

Directory Access rules are applied in the order they are listed. The first rule Serv-U encounters in the list that matches the path of a client's request is the one that's applied for that rule. In other words, if a rule exists that denies access to a particular subdirectory but is listed below the rule that grants access to the parent directory, then a User still has access to the subdirectory in question. The arrows on the right side of the Directory Access list are used to re-arrange the order in which the rules are applied.

A listing and description of each available directory access permission follows.




# File Permissions

## Read

Allows Users to read, (i.e., download) files. This permission does not allow Users to list the contents of a directory, which is granted by the List permission.

## Write

Allows Users to write, (i.e., upload) files. This permission does not allow Users to modify existing files, which is granted by the Append permission.

## Append

Allows Users to append data to existing files. This permission is normally used to grant Users the ability to resume transferring to partially uploaded files.

## Rename

Allows Users to rename existing files. Previous versions of Serv-U required Delete and Write permissions to rename files. Starting with version 7.0, Rename is an explicit permission.

## Delete

Allows Users to delete files.

### Execute

Allows Users to remotely execute files. Execute access is meant for remotely starting programs and usually applies to specific files. This is a very powerful permission and great care should be used in granting it to Users. A User with Write and Execute permissions can essentially install any program of their choosing on your system.

## Directory Permissions

### List

Allows Users to list the files contained in the directory.

### Create

Allows Users to create new directories within the directory.

### Rename

Allows Users to rename existing directories within the directory. Previous versions of Serv-U required Delete and Write permissions to rename directories. Starting with version 7.0, Rename is an explicit permission.

### Delete

Allows Users to delete existing directories within the directory. NOTE: If the directory contains files, the User also needs to have the Delete files permission in order to delete the directory.

## Subdirectory Permissions

### Inherit

Allows all subdirectories to inherit the same permissions as the parent directory. The Inherit permission is appropriate for most circumstances, but if access must be restricted to subdirectories (as is the case when implementing Mandatory Access Control), uncheck Inherit and grant permissions specifically by folder.

## Access as Windows User

For a variety of reasons, files and folders may be kept on external servers in order to centralize file storage or provide additional layers of security. In this environment, files can be accessed by UNC path (\\servername\folder\) instead of the traditional "C:\ftproot\folder" path. However, accessing folders stored across the network poses an additional challenge - Windows services are run under the "Local System" account by default, which has no access to network resources.

To mitigate this problem for all of Serv-U, it is possible to configure the "Serv-U File Server" service to run under a network account. The alternative, preferred when many servers exist or if the Serv-U File Server service needs to run under "Local System" for security reasons is to configure a Directory Access rule to use a specific Windows User for file access. By clicking on the "Advanced" button it is possible to specify a specific Windows user for each individual Directory Access rule. Just like in Windows Authentication, directory access is subject to NTFS permissions, though in this case also to the configured permissions in Serv-U.

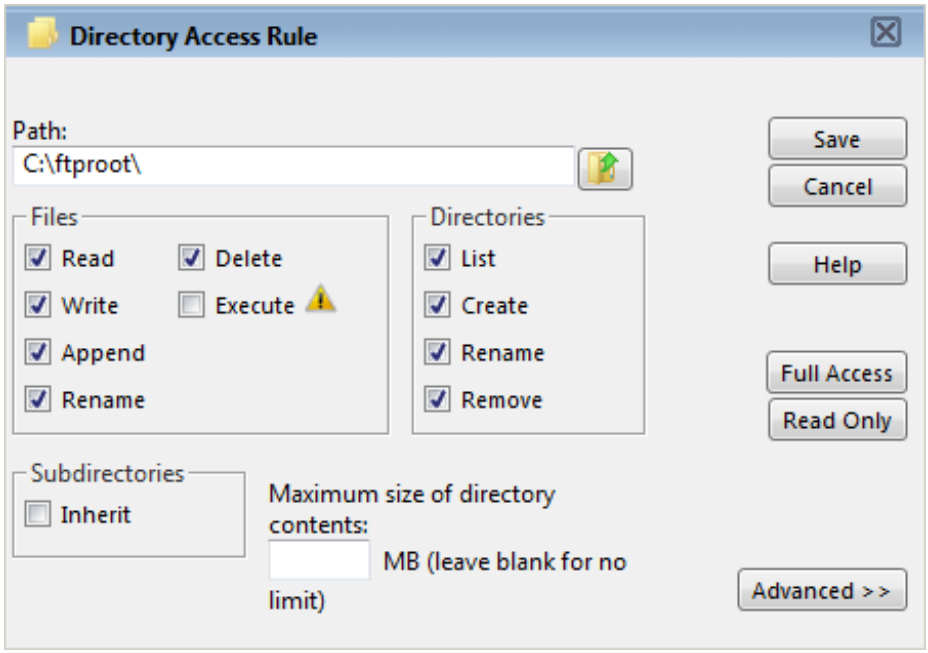
# Quota Permissions

## Maximum size of directory contents

Setting the maximum size actively restricts the size of the directory contents to the specified value. Any attempted file transfers that cause the directory contents to exceed this value are rejected. This feature serves as an alternative to the traditional quota feature that relies upon tracking all file transfers (uploads and deletions) to calculate directory sizes and is not able to consider changes made to the directory contents outside of a User's File Server activity.

# Mandatory Access Control

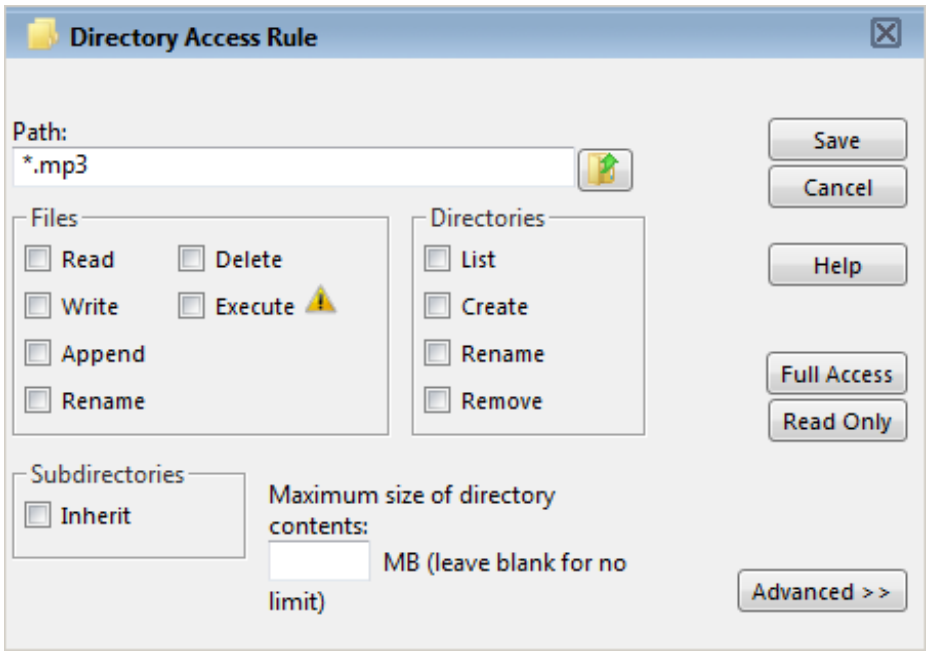
Serv-U enables the use of Mandatory Access control in cases where Users need to be granted access to the same home directory but should not be able to necessarily access the subdirectories below it. To implement Mandatory Access Control at a directory level, simply disable the "Inherit" permission as shown below (assume the rule applies to "D:\ftproot\"):



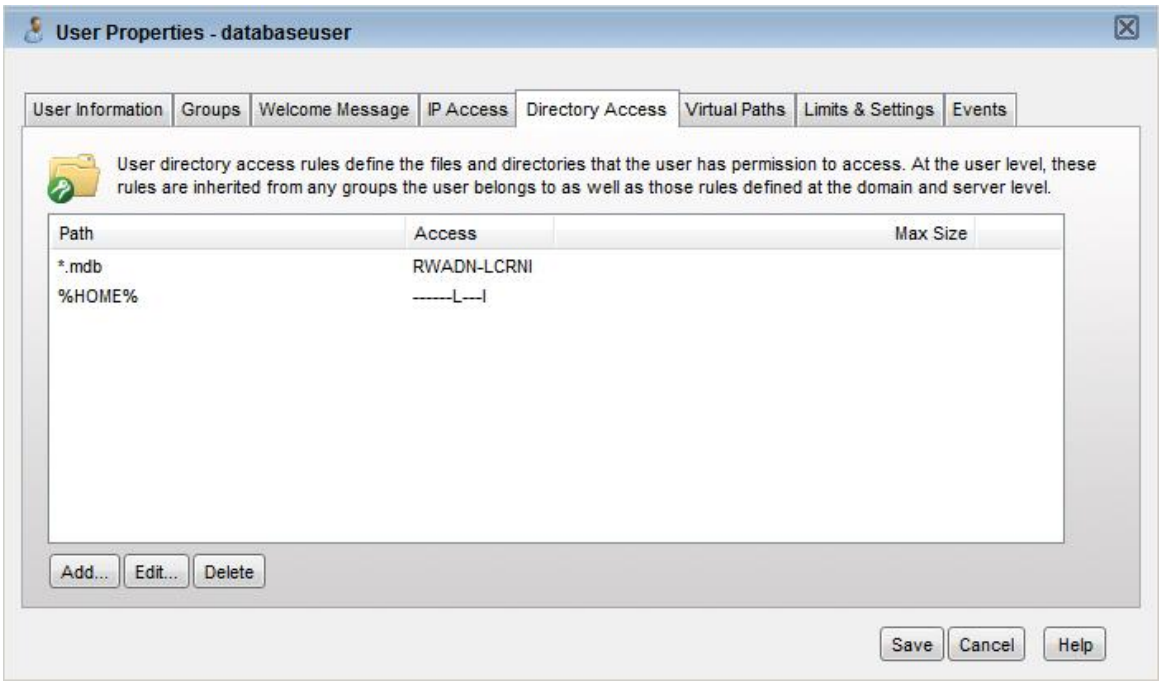

Now, the user has access to the "ftproot" folder but to no folders below it. Permissions must individually be granted to subdirectories that the user needs access to, providing the security of Mandatory Access Control in the Serv-U File Server.

# Restricting File Types

If Users are using storage space on the Serv-U File Server to store non-work-related files such as MP3 music files, this can be prevented by configuring a Directory Access rule placed above the main Directory Access Rule (use the arrows on the right to reorder rules) to prevent MP3 files from being transferred as shown below. In the text entry for the rule, enter "*.mp3" and use the permissions shown below:



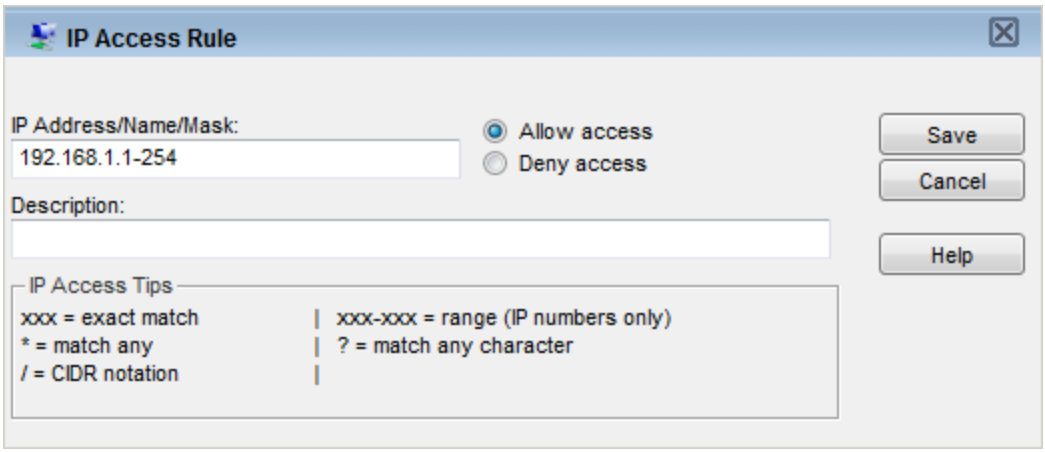

The rule denies permission to any transfer of files with the .mp3 extension and can be modified to reflect any file extension. Similarly, if accounting employees only need to transfer files with the .mdb extension, configure a pair of rules that grants permissions for .mdb files but denies access to all other files, as shown below. In the first rule enter the path that should be the user's home directory or directory they need access to, and in the second rule enter the extension of the file that should be accessed (such as "*.mdb"):



# IP Access Rules

IP Access rules are an additional form of user authentication that can restrict login access to specific IP addresses, ranges of IP addresses, or even a domain name. IP Access rules can be configured at the Server, Domain, Group, and User levels. The level at which an IP access rule is specified also defines how far a connection is allowed before being rejected. Server and Domain level IP access rules are applied before the Welcome message is sent. Domain level IP access rules are also applied when responding to the HOST command to connect to a virtual domain. Group and User level IP access rules are applied in response to a USER command when the client identifies itself to the server.

Specifying these rules ensures that only clients in certain networks can log in. To configure IP Access rules, first specify what clients are allowed to log in or not allowed to log in. Add rules by clicking the Add button and specifying what IP addresses or range of addresses are to be applied to the rule. If a dynamic DNS service is used, then a domain name can be specified in place of an IP address to allow access to clients that travel and don't have a static IP address. Reverse DNS names are also acceptable. If a domain name or reverse DNS rule is created, Serv-U must perform either a reverse DNS look-up or DNS resolution in order to apply these rules. This can cause a slight delay during login depending upon the speed of the system's DNS server.




Special formatting allows ranges and wildcards to be used, as below:

## Specific IP - xxx

An exact match such as 192.168.1.1.

## Range - xxx-xxx

A specified range of IP addresses such as 192.168.1.10-19.

## Wildcard - *

Any valid IP address value such as 192.168.1.*, which is analogous to 192.168.1.0-255.

## Mask - ?

Any valid character when specifying a reverse DNS name such as server?.mydomain.com.

## CIDR Block - /

The slash separator allows the use of CIDR notation to specify which IP addresses should be allowed or blocked. Common CIDR blocks are /8 (for 1.*.*.*), /16 (for 1.2.*.*) and /24 (for 1.2.3.*). The block /32 can be used to specify a single IP address.

IP access rules are applied in the order they are displayed. In this way, specific rules can be placed at the top to allow (or deny) access before a more general rule is applied later on in the list. The arrows on the right side of the list can be used to change the position of an individual rule in the list.

Approved addresses already appearing in the list do not become automatically blocked by the anti-hammering rule. For example, a local IP address 192.168.0.17 causes Serv-U to initiate its anti-hammer rule to ban the IP address, but 192.168.0.17 is explicitly approved in the list, 192.168.0.17 is not automatically blocked by the anti-hammer rule.

Here's how it works. Assuming the following IP access rules:

+ 192.168.0.17
+ *

When there's activity coming from 192.168.0.17, but the user gets the password wrong auto IP blocking (via timeout, anti-hammer, or by system admin from Sessions Activity) doesn't occur because that IP address is specifically enabled. The bottom item * means everyone is approved, without this value only 192.168.0.17 would be approved. If anti-hammer kicks in for a different IP address the blocked IP address gets added to the top of the list, so it looks like:

- 10.10.10.1
+ 192.168.0.17
+ *

If an entire block of IP addresses is desired, this also works as described:

+ 192.168.0.1-255
+ *

If anti-hammer kicks in on any of these IPs, the IP is not blocked. The key here is the wild card *. Serv-U also checks for *.*, *.*.*, *.*.*.* as being "any" IP address.

## IPv6 Support

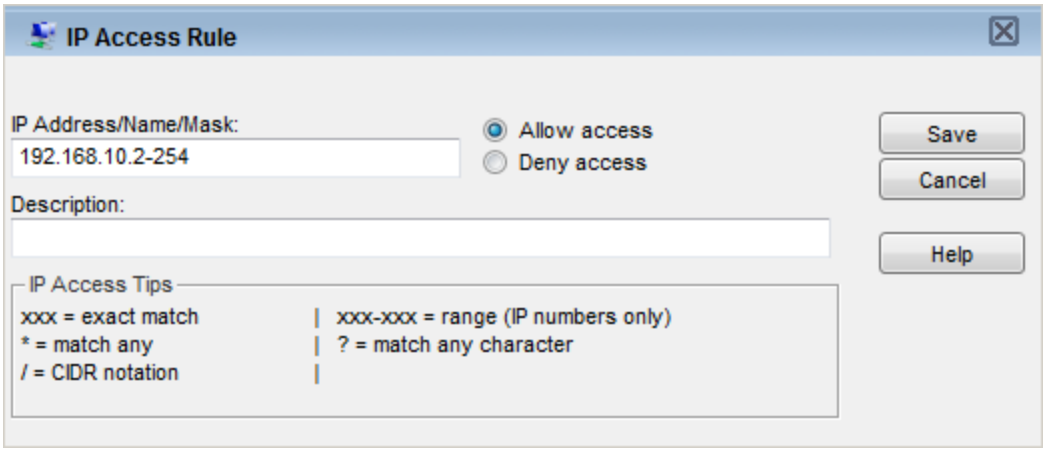
Serv-U also supports IP Access rules based on IPv6 address ranges in CIDR notation. As with IPv4, the number after the slash indicates which addresses are considered a part of the range, such as 2001:db8::/32.

## Enable Sort Mode

This option allows the IP Access list to be sorted numerically rather than in the processing order. Displaying the IP Access list in sort mode will not change the order in which rules are processed - to view rule precedence disable this option. Viewing the IP Access list in numerical order can be a valuable tool when reviewing long lists of access rules to determine if an entry already exists.

## Case File - Contractor

A contractor has been hired on a temporary basis, and access to the Serv-U File Server is required for the contract work to be completed effectively. He is granted access but should not be able to access the Server from locations outside of the field office as it would pose a risk to confidentiality. All of the in-office workstations are assigned IP addresses from 192.168.10.2-192.168.10.254. Therefore, create an Allow Access rule as shown:




The rule shown above permits the contractor to access the file server from inside the office, but because of the creation of the "Allow Access" rule there is an implicit "Deny All" rule added that prevents the account from being used anywhere else. He is granted the access necessary for the position, but the administrator has greater control over where the data is accessed.

## Case File - Open Kiosks

A user needs to be able to access the Server from within the office, but should not be able to log on from a set of open PC kiosks in the building for security reasons. The kiosks are assigned IP addresses from 192.168.15.100-192.168.15.110. Therefore, create a Deny Access rule which denies access to 192.168.15.100-192.168.15.110. Keep in mind that because of the implicit "Deny All" rule added when using IP Access rules, an "Allow All" rule must be added at the end of the list to allow the

user to log on from all other address ranges by entering an Allow Access rule which allows access to "*.*.*.*". This rule at the end ensures that connections are allowed from all other IP addresses.

## Case File - Access By Name

Users connecting from the examplesite.com Domain should be the only ones able to access the Domain. To restrict the users able to connect to the Domain, implement an IP Access rule based on reverse DNS and host name. First, create a new access rule allowing access to *.examplesite.com at either the User or Group level. Then, if the rule is set at the Group level, add all relevant users to the Group so that the rule is applied to them. DNS based IP Access rules cannot be set at the Domain or Server levels because they take more time to resolve than IP address IP Access rules and setting them at these levels potentially slow other logins.

NOTE: For such an access rule to work, the PTR records for the IP addresses in question must match the rule that has been created. Generally, the connecting clients must be connecting from a large company with an IP range assigned to it for the connecting IP addresses to have such PTR records - typically, dynamic IP addresses do not meet the requirement.

# Limits & Settings

Serv-U offers advanced options which can be used to customize how it may be used as well as ways to apply limits and custom settings to **Users**, **Groups**, **Domains**, and the **Server** in its entirety. The limits stack intelligently, with User settings overriding Group settings, Group settings overriding Domain settings, and Domain settings overriding Server settings. In addition, limits can be applied only during certain days of the week or times of the day. It is possible to grant exceptions to administrators and restrict specific Users more than others, providing total control over the Server. The Limits and Settings in Serv-U are split into five categories: **Connection**, **Password**, **Directory Listing**, **Data Transfer**, and **Advanced**.

To apply a limit, select the appropriate category, click on the **Add** button, select the limit, then select or enter the value. For example, to disable the **Lock users in home directory** option for a Domain, follow these steps:

- Select Domain Limits & Settings link from the Serv-U Management Console.
- Select **Directory Listing** from the "Limit Type" drop-down box.
- Click the **Add** button.
- Select **Lock users in home directory** from the "Limit" drop-down box.
- Uncheck the option.
- Click the **Save** button.

The limits list displays the current limits applied to the domain. Limits with a light-blue shade to the background are default values. Limits with a white background are values that override the defaults. After completing the above steps, a new **Lock users in home directory** limit appears in the list that displays "No" for the value. Because of inheritance rules, this option applies to all users in the domain unless overridden at the Group or User level.

Limits can be deleted by selecting them and clicking the **Delete** button. To edit an overridden value, select the limit and click the **Edit** button. Default rules cannot be edited or deleted. Create a new limit to override a default one.

To create a limit that is restricted to a specific time of day or days of the week, click the **Advanced** button from the New / Edit Limit dialog. The additional options allow you to **Apply limit only at this time of day** at which point a start and stop time for the new limit can be entered. To restrict the limit to certain days of the week, uncheck the boxes next to the days you don't want the limit applied. When a limit is restricted in this way, default values (or the value of other limit overrides) are applied when the time of day or day of the week restrictions are not met for this limit.

The following is a reference of all available **User** limits, organized by category.

## Connection

### Block anti-timeout schemes

Blocks the use of commands such as "NOOP", which is commonly used to keep FTP Command Channel connections open during long file transfers or other periods of inactivity where no information is being transferred on the control channel. When these are blocked, Serv-U disconnects the client when the connection has been idle, i.e., not transferring data, for a specified period of time.

## Automatic idle connection timeout

Specifies the number of minutes that must pass after the last client data transfer before a session is disconnected for being idle.

## Maximum sessions per IP address for user account

Specifies the maximum number of concurrent sessions that a User may open from a single IP address.

## Maximum number of sessions per user account

Specifies the maximum number of concurrent sessions that may be opened from a single User account.

## Require secure connection before login

Requires that a connection be secure, (e.g., FTPS, SFTP, or HTTPS), before it is accepted.

## Automatic session timeout

Specifies the number of minutes a session is allowed to last before being disconnected by the Server.

## Block IP Address Of Timed Out Session

Specifies the number of minutes for which the IP address of a timed out session is blocked.

## Allow FTP and FTPS Connections

Allows the user to connect using the FTP and FTPS protocols. Uncheck "Allow FTP and FTPS connections" to disable the FTP and FTPS protocols.

## Allow SFTP Connections

Allows the user to connect using the SFTP protocol. Uncheck "Allow SFTP connections" to disable the SFTP protocol.

## Allow HTTP and HTTPS Connections

Allows the user to connect using the HTTP and HTTPS protocols. Uncheck "Allow HTTP and HTTPS connections" to disable the HTTP and HTTPS protocols.

# Password

## Require complex passwords

Specifies that all User account passwords must contain at least one uppercase and one non-alphabetic character to be considered valid.

## Minimum password length

Specifies the minimum number of characters required in a User account's password. Specifying 0 characters indicates that there is no minimum requirement.

## Automatically expire passwords

Specifies the number of days a password is valid before it must be changed. Specifying 0 days means passwords never expire.

## Allow users to change password

Specifies whether or not Users are allowed to change their own passwords.

## Mask received passwords in logs

Masks the passwords received from clients from being shown in log files. Disabling this allows passwords to be displayed in log files, which can be useful for debugging connection problems or auditing User account security.

## FTP Password Type

All passwords are stored in an encrypted, irreversible state in Serv-U's configuration files (unless the File Server is configured to not encrypt stored passwords through Password Limits). In addition to the **Regular Password** option, two additional types of password storage are available for accounts that use the FTP protocol: **MD4** and **MD5** OTP S/KEY passwords. This type of password setting allows the user to login via FTP without sending the password to the File Server as plain text. These options only apply to the FTP protocol. Setting this option does not affect a User's ability to login via other protocols.

## SSH authentication type

Specifies how SSH authentication is to occur. Options include: "Password and Public Key" - requires both a password and a public key (when specified) for login; "Password or Public Key" - requires either a password or public key for login; "Public Key Only" - requires that a public key is provided for successful login, a password is not allowed; "Password Only" - requires that a password is provided for successful login, a public key is not allowed.

## Allow users to recover password

If enabled, allows users to recover passwords using the Web Client password recovery utility at the login page.

# Directory Listing

## Hide files marked as hidden from listings

Hides files and folders from directory listings that have the Windows "hidden" system attribute set on them.

## Use lowercase for file names and directories

Forces Serv-U to display all file names and directories using lowercase characters, regardless of the actual letter case in use by the file or directory.

## Allow root ("/") to list drives for unlocked users

Allows Users to change directory to the root ("/") of the system and display all drives on the computer. This option only works when the User is not locked in their home directory.

## Treat Windows shortcuts as target in links

Instructs Serv-U to treat all valid .lnk (shortcut) files as a UNIX symbolic link.

## Hide the compressed state of files and directories.

Hides the compressed state of all compressed files and directories being viewed by the user.

## Hide the encrypted state of files and directories.

Hides the encrypted state of all encrypted files and directories being viewed by the user.

## Interpret Windows shortcuts as links

Instructs Serv-U to treat all valid .lnk files as the actual destination object. In other words, if a .lnk file points to another file, the destination file is shown in the directory listing instead of the .lnk file itself.

# Data Transfer

## Delete partially uploaded files

Instructs Serv-U to delete incomplete file uploads. If this option is enabled, Users are not able to restart interrupted uploads using the REST (Restart) FTP command.

## Maximum download speed per session

Limits the maximum download bandwidth for each individual session. Setting a limit of 0 KB/s means unlimited bandwidth.

## Maximum upload speed per session

Limits the maximum upload bandwidth for each individual session. Setting a limit of 0 KB/s means unlimited bandwidth.

## Maximum download speed for user accounts

Limits the maximum download bandwidth shared between all sessions associated with an individual User account. Setting a limit of 0 KB/s means unlimited bandwidth.

## Maximum upload speed for user accounts

Limits the maximum upload bandwidth shared between all sessions associated with an individual User account. Setting a limit of 0 KB/s means unlimited bandwidth.

## Maximum Upload File Size

Restricts the maximum single file size a user can upload to Serv-U. File size measured in kilobytes.

## Interpret line feed byte as a new line when in ASCII mode

When uploading and downloading files using ASCII mode, Serv-U will assume <LF> characters are the same as <CR><LF> end-of-line markers. Most Windows applications expect <CR><LF> to represent a new-line, as does the FTP protocol. However, since the definition of a new-line sequence is not fully defined in Windows, this option allows Serv-U to assume <LF> is the same as <CR><LF>. When uploading in ASCII mode stand-alone <LF> characters are changed to <CR><LF> prior to writing to the file. When downloading in ASCII mode, stand-alone <LF> characters are changed to <CR><LF> prior to sending to the client.

# HTTP

## Default language for Web Client

When the end-user connects with an unsupported language, the HTTP Login Page is displayed in English. The default language can be set to any desired language. When connecting to Serv-U using a supported localization of Windows, the native language of Windows is used.

## Allow HTTP media playback

The Serv-U Web Client supports fully interactive media playback of audio and video files. This function can be disabled as desired during specific business hours or altogether based on business needs.

## Allow the users browser to remember login information

The HTTP login page supports a "Remember me" option (not enabled by default) that allows usernames to be remembered by the login page. This feature can be disabled for security reasons.

## Allow users to change themes

The Serv-U Web Client supports visual themes to change the look and feel of the Web Client and HTTP login page. This feature is visual only and has no impact on security or functionality. This option can be disabled for business needs.

## Allow users to change languages

The Serv-U Web Client is supported in many languages, but if users should not be able to select their native language this can be disabled.

# Advanced

## Automatically check directory sizes during upload

Instructs Serv-U to occasionally check the size of directories in which a maximum directory size has been specified. This attribute ensures that Serv-U always has updated directory sizes available instead of having to calculate them at transfer time, which can be a time consuming operation.

## Convert URL characters in commands to ASCII

Instructs Serv-U to convert special characters contained in command parameters to plain ASCII text. Certain Web browsers can encode special characters contained in file names and directories when using the FTP protocol. This attribute allows Serv-U to decode these special characters.

## Maximum Supported SFTP Version

Specifies the maximum version of SFTP permitted for SFTP connections. Serv-U supports SFTP versions 3-6.

## Warn end users when using old web browsers

When enabled (default) Serv-U allows files to be renamed to files where the destination already exists. When disabled users are not allowed to rename a file or directory to a path name that already exists.

# Domain Settings

## Block users who connect more than 'x' times within 'y' seconds for 'z' minutes

Also known as anti-hammering, enabling this option is a method of preventing brute force password guessing systems from using dictionary style attacks to locate a valid password for a user account. Using strong, complex passwords defeats most dictionary attacks. However, enabling this option ensures that Serv-U does not waste time processing connections from these illegitimate sources. When configuring this option, ensure that there is some room available for legitimate users to correct an incorrect password before they are blocked.

When enabled, this option temporarily blocks IP addresses for 'z' minutes that fail to successfully login after 'x' attempts within 'y' seconds. IP addresses blocked in this way can be viewed in the appropriate IP Access rules tab. A successful login resets the counter tracking attempted logins.

## Hide server information from SSH identity

After a successful SSH login, the server sents identification information to the client. Normally, this information includes the server name and version number. Enable this option to prevent the information from being given to the client.

## Default Web Client

Specifies whether the Web Client or FTP Voyager JV should be used by all HTTP clients by default. A third option (the default option) is to prompt the User for the client they want to use instead. This option is also available at the Group and User level.

## Client Support Link

The Client Support Link is a powerful feature that allows a direct method of contact to be inserted into the Web Client and FTP Voyager JV in the event that a client requires support or assistance. The basic syntax for this feature is **protocol:path**. This option is highly flexible and allows for any network shortcut to be used, such as:

http://www.website.com/support/

**mailto:service@website.com?subject=Serv-U File Server Support**

**aim:goim?screenname=ExampleAdminUser&message=I need help with your Serv-U File Server!**

Any format can be used as long as the client's machine understands the provided protocol.

# Transfer Ratio and Quota Management

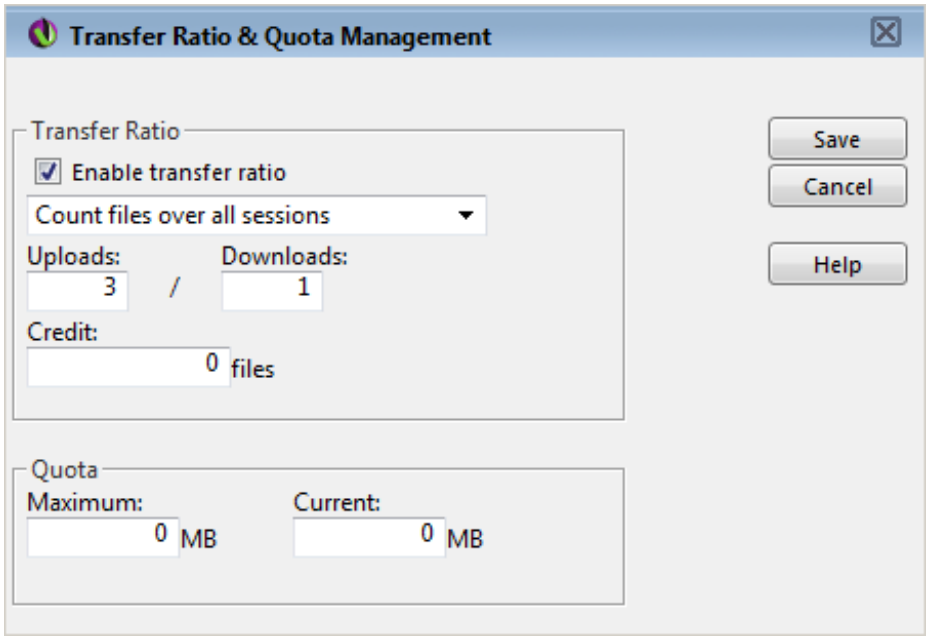
Transfer Ratios and Quotas are just one of the many ways in which file transfers are managed on the Serv-U File Server. For more information on each of these options, continue reading.

## Transfer Ratio

Transfer ratios are a convenient way of encouraging file sharing on your File Server. By specifying an appropriate transfer ratio setting, you can grant "credits" to the User for transferring a specified number of bytes or complete files. This is commonly used to grant a User the ability to download 'x' megabytes of data or files for every 'y' megabytes of data or files that they upload.

To enable transfer ratios for the current User account, check the box labeled Enable transfer ratio. Select the appropriate type of ratio to impose on the User account. Ratios can be tracked in terms of megabytes or complete files. They can also be tracked per session established or for all sessions established by the User account.

The ratio itself is configured by assigning a numeric value to both the Uploads and Downloads side of the ratio. For example, a 3/1 ratio that is counting files over all sessions means that the User account must upload 3 files in order to have the ability to download 1 file. The current credit for the User account is displayed in the Credit field. This value is the current value and can be initialized to a non-zero value to grant the User initial credits.



## Quota

Quotas are another way to limit the amount of data that is transferred by a User account. When a Maximum quota value is assigned to the User, they are not able to use more disk space than that value. The Current field shows how much disk space is currently being used by the User account. When initially configuring a quota, both fields must be filled in. From that point on, Serv-U tracks the file uploads and deletions made by the User and updates the Current value as appropriate.

NOTE: One considerable drawback to using quotas is that in order for the Current value to remain accurate, changes must not be made to the contents of the directories that are accessible by the User account outside of Serv-U. Because these changes take place outside of a File Server connection, Serv-U cannot track them and update the current quota value. As an alternative to quotas, consider imposing a maximum size on the contents of a directory when specifying the Directory Access rules for the User account. For more information on this option, see the Help documentation on Directory Access Rules.

## Ratio Free Files

Files listed in the ratio free file list are exempt from any imposed transfer ratios. In other words, if a User must upload files in order to earn credits towards downloading a file, a file that matches an entry in this list can always be downloaded by Users, even if they have no current credits. This is commonly used to make special files, such as a "read me" or a directory information file, always accessible by Users.

The '*' and '?' wildcard characters may be used when specifying a ratio free file. Using '*' specifies a wildcard of any kind of character and any length. For example, entering "*.txt" makes any file with a .txt extension free for download, regardless of the actual file name. A '?' may be used to represent a single character within the file name or directory.

In addition, full or relative paths may be used when making an entry. If a full path is used when specifying a file name, then only that specific file is exempt from transfer ratios. If a relative path is used, such as entering just "readme.txt", then the provided file is exempt from transfer ratios regardless of the directory it is located in.

# Virtual Hosts

Virtual Hosts provide a way for multiple Domains to share the same IP and Listener port numbers. Normally, each domain listener must use a unique IP address and port number combination. With Virtual Hosts, it's possible to host multiple Domains on a system that only has one unique IP address without having to use non-standard port numbers. The Domains can share the same listeners by proper implementation of Virtual Hosts. This feature is only available when the current license supports hosting multiple Domains.

To configure Virtual Hosts for a Domain, click on the Add button and type in the Virtual Host name for the Domain. The Virtual Host name is usually the fully qualified domain name used to connect to the Domain such as "ftp.Serv-U.com".

The method used by a client to connect to a desired Virtual Host depends upon the protocol being used to connect to Serv-U.

FTP
FTP users can use one of two methods to connect to a specific Virtual Host. If supported by the FTP client, the HOST command can be issued to Serv-U before login to identify the Virtual Host. Otherwise, the virtual host can be provided with the login ID in the following format: virtual_host_name|login ID. The Virtual Host name is entered first, followed by the vertical bar character ('|'), then the login ID.

SFTP
SFTP users wishing to connect to a specific virtual host must use the specially crafted login ID format as described above in the FTP section.

HTTP
For HTTP users, the browser automatically provides Serv-U with the hostname used to reach the site allowing Serv-U to identify the Virtual Host from the fully qualified domain name entered into the browser's navigation bar.

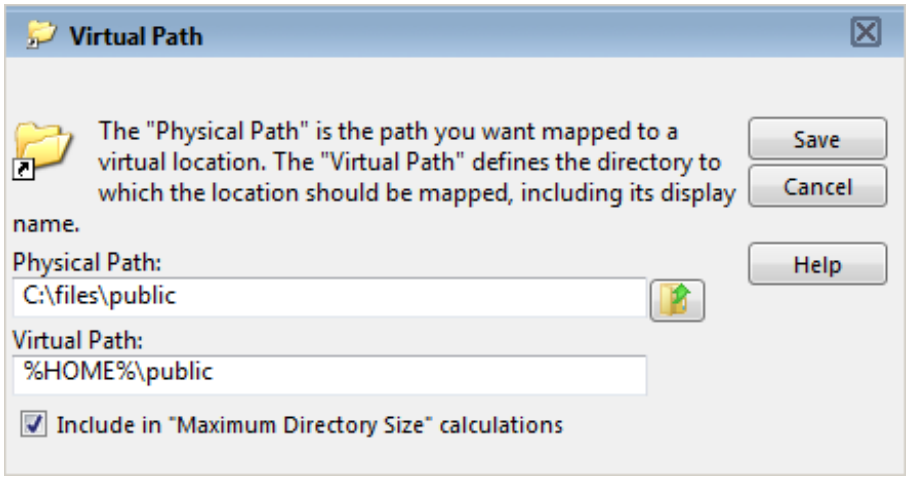
## Case File - Virtual Hosts

Multiple Domains are being configured on the same Server, which has one IP address and two Fully Qualified Domain Names (FQDN) pointing to it. Because Users connecting to both Domains must use port 21 for connections, configure Virtual Hosts on each Domain so that Serv-U can distinguish between requests for the two Domains. After setting up the same listener properties on each Domain, open the Virtual Hosts tab, click Add, and then type in the FQDN that clients should use to connect to the Domain.

After connecting to the Server with FTP, Users can send a HOST ftp.Serv-U.com command to connect to the appropriate Domain on the File Server. FTP and SFTP users could also identify the Virtual Host through their login ID of ftp.Serv-U.com|login ID. If connecting via HTTP, Users can connect to this Domain by visiting http://ftp.Serv-U.com.

# Virtual Paths

Virtual Paths allow Users to gain access to files and folders outside of their own home directory. A Virtual Path only defines a method of mapping an existing directory to another location on the system to make it visible within a User's accessible directory structure. In order to actually have access to the mapped location, the User must still have a Directory Access rule specified for the physical path of a Virtual Path.




Like Directory Access Rules, Virtual Paths can be configured at the Server, Domain, Group, and User levels. Virtual Paths created at the Server level are available for use by all Users of the File Server. When created at the Domain level, they are only accessible by Users belonging to that Domain. Serv-U's granular file access controls even allow for Virtual Paths created specifically for individual Users or Groups.

## Physical Path

The physical path is the actual location on the system, or network, that is to be placed in a virtual location accessible by a User. If the physical path is located on the same computer, a full path should be used, such as "D:\inetpub\ftp\public". A UNC path can also be used, such as "\\Server\share\public". In order for a Virtual Path to be visible to a User, they must have a Directory Access rule specified for the physical path.

## Virtual Path

The virtual path is the location that the physical path should appear in for the User. The %HOME% macro is commonly used in the virtual path to place the specified physical path in the home directory of the User. When specifying the virtual path, the last specified directory is used as the name displayed in directory listings to the User. For example, a virtual path of "%HOME%/public" places the specified physical path in a folder named "public" within the User's home directory. A full path without any macros can also be used.

## Include in "Maximum Directory Size" calculations

When checked, the Virtual Path is included in Maximum Directory Size calculations. When unchecked, the Virtual Path is not included in the Maximum Directory Size calculations. Maximum Directory Size limits the size of directories affecting how much data can be uploaded.

## Case File - Using Virtual Paths

A Group of web developers have been granted access to the directory "D:\ftproot\examplesite.com\" for web development purposes. The developers also need access to an image repository located at "D:\corpimages\". To avoid granting the Group access to the root D drive, a Virtual Path must be configured so that the image repository appears to be contained within their home directory. Within the web developer's Group, add a Virtual Path to "bring the directory to the users" by specifying "D:\corpimages\" as the Physical Path and "D:\ftproot\examplesite.com\corpimages" as the Virtual Path. Be sure to add a Group level Directory Access rule for "D:\corpimages\" as well. The developers now have access to the image repository without compromising security or relocating shared resources.

## Case File - Creating Relative Virtual Paths

Continuing with the example from above, if the web developer's Group home directory is relocated to another drive, not only does the home directory have to be updated, but the Virtual Path also needs to be updated to reflect this change. This can be avoided by using the %HOME% macro to create a relative Virtual Path location that eliminates the need to update the path should the home directory change. Instead of using "D:\ftproot\examplesite.com\corpimages" as the Virtual Path, use "%HOME%\corpimages". This tells Serv-U to place the "corpimages" Virtual Path within the Group's home directory - whatever that may be. If the home directory changes at a later date, the Virtual Path still appears there.

# Groups

Groups are a method of sharing common configuration options with multiple User accounts. Configuring a Group is just like configuring a User account. Virtually every configuration option available for a User account can be set at the Group level. In order for a User to inherit a Group's settings, it must be a member of the Group. Permissions and attributes inherited by a User through Group membership can still be overridden at the User level. A User can be a member of multiple Groups in order to acquire multiple collections of permissions, such as directory or IP access rules.

Like User accounts, Groups can be created at multiple different levels, including:

- Global Groups
- Domain Groups
- Database Groups - available at both the Server and Domain levels

However, Groups are only available to User accounts that are defined at the same level. In other words, a Global User, (i.e., a User defined at the Server level), can only be a member of a Global Group. Likewise, a User defined for a specific Domain can only be a member of a Group also created for that Domain. This restriction also applies to Groups created in a database in that only Users created within a database at the same level can be members of those Groups.

Use the Add, Edit, and Delete buttons to manage the available Groups.

## Group Template

Serv-U allows an administrator to configure a template for creating new Groups by clicking on the Template button. Once opened, the template Group can be configured just like any other Group object, with the exception of giving it a name. After these settings are saved to the template, all new Groups are created with their default settings set to those found within the template. This is a great way to configure some basic settings that you want all of your Groups to use by default to save you time when creating new Groups.

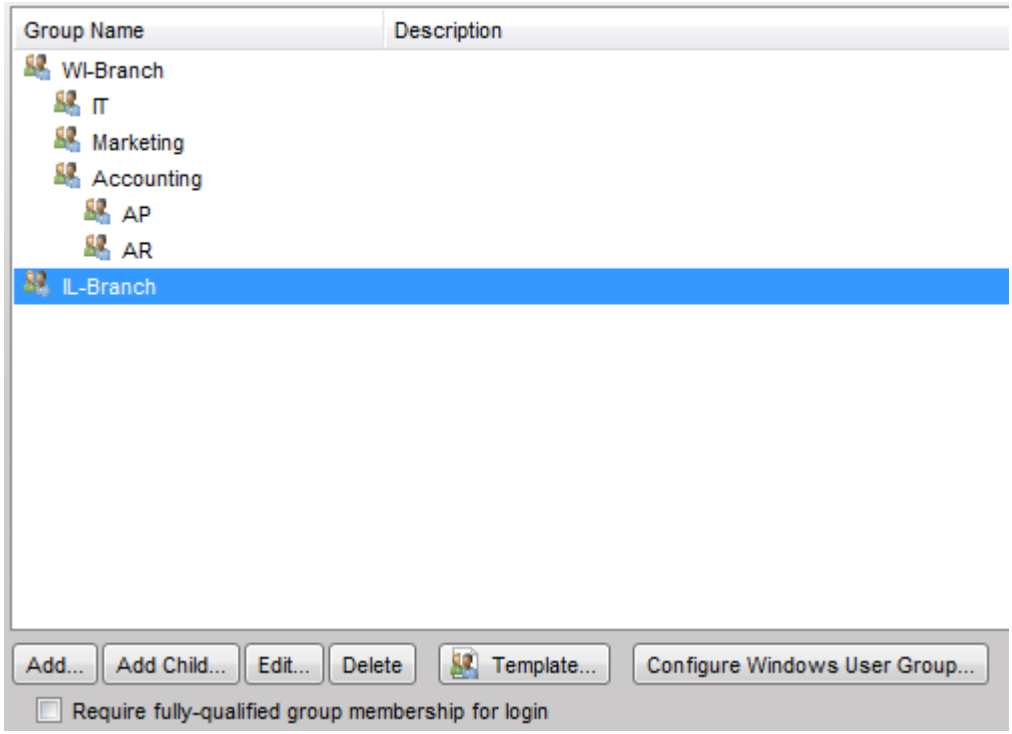
## Configure Windows User Group

Administrators have the ability to allow clients to login to the File Server using the local Windows user database or one that is made accessible through a domain server. These User accounts do not exist in the local Serv-U User database and cannot be configured on an individual basis. To aid in configuring these accounts, all Users logged in through this method belong to the Default Windows User Group. Clicking this button allows this Group to be configured like normal. However, changes that are made to this Group only apply to Windows User accounts.

# Serv-U Windows Groups

Serv-U includes full support for Active Directory by allowing administrators to configure individual Organization Units with different permissions and settings, even restricting Serv-U logon to certain OUs. To simplify the process, the new Serv-U Windows Groups are configured in a heirarchical structure just like OUs in Active Directory.

In Serv-U, Windows Groups are configured in the "Groups | Windows Groups" menu. To enable this option, Windows Authentication must first be enabled in the "Users | Windows Authentication" menu. After the Active Directory Domain Name is provided, click "Save" and open the "Groups | Windows Groups" menu.



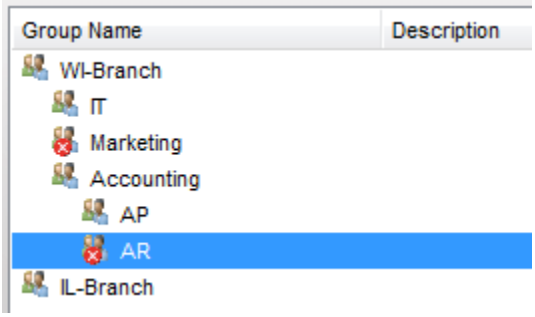

**NOTE:** To require membership in a listed OU, enable the "Require fully qualfied group membership for login" option.

The generic Windows User Group can still be configured as before using the "Configure Windows User Group" option, but the groups list above is where Serv-U's new functionalty shines through. To define Organizational Units in Serv-U, start with the Organizational Unit that is the parent in your AD structure (the root of your Active Directory Domain). In this case, our Active Directory is sorted by branch, with the root Domains being the state-wide branches (WI-Branch and IL-Branch). Within WI-Branch we have defined the different departments that are allowed to log in to Serv-U.

## Adding Windows Groups

- Adding Windows Groups is easy, following the steps outlined below:
- Click "Add" to add any root groups, starting at the root of your AD Domain.

- To add children OUs, click the parent OU and then click "Add Child" to define the OUs you desire to configure in the same structure and heirarchy as your Active Directory.
- To edit the individual OUs, use the "Edit" button. Each OU can have its own Virtual Paths, bandwidth limits, and more. You can even enable/disable individual OUs from logging on to Serv-U as necessary




- By default, all Windows users may log on. To change this, click "Require fully qualified group membership for login" so that only approved Windows users may log on.

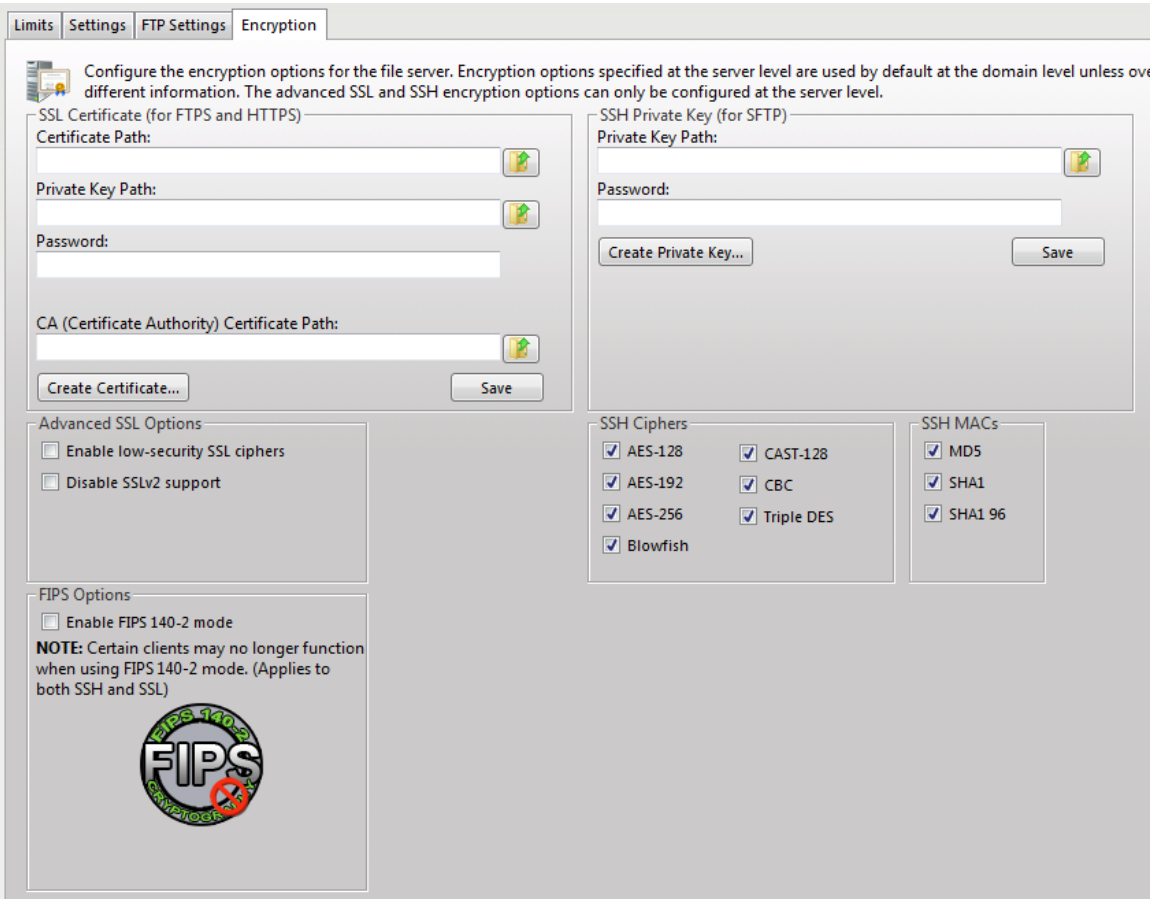
Using Windows Groups in Serv-U 10 allows administrators to fully control individual OUs, defining within Active Directory who may and may not log on to Serv-U as well as what permissions they may have outside of their standard NTFS permissions.

# Encryption

Serv-U supports two methods of encrypted data transfer - Secure Socket Layer (SSL) and Secure Shell 2 (SSH2). SSL is used to secure the File Transfer Protocol (FTP) and Hypertext Transfer Protocol (HTTP). SSH2 is a method of securely interacting with a remote system that supports a method of file transfer commonly referred to as SFTP. Despite its name, SFTP does not have anything in common with the FTP protocol itself.

In order for each method of encryption to work, a certificate and/or private key must be supplied. SSL requires the presence of both, while SSH2 only requires a private key. If you do not possess either of these required files, Serv-U can create them for you.

Encryption options specified at the Server level are automatically inherited by all Domains. Any encryption options specified at the Domain level automatically overrides the corresponding Server-level option. Certain configuration options are only available to the Server.




When creating SSL/TLS, SSH, and HTTPS encrypted Domains within Serv-U, it is important to know that encrypted Domains cannot share listeners. Because SSL/TLS and SSH encryption is based on encrypting traffic sent between IP addresses, each Domain must have unique listeners in order to operate properly. In the case that multiple encrypted Domains are created that share listeners, the

Domain created first takes precedence causing other encrypted Domains to fail to function properly. To operate multiple encrypted Domains, modify the listeners of each Domain to ensure they listen on unique port numbers.

# Configuring SSL for FTPS and HTTPS

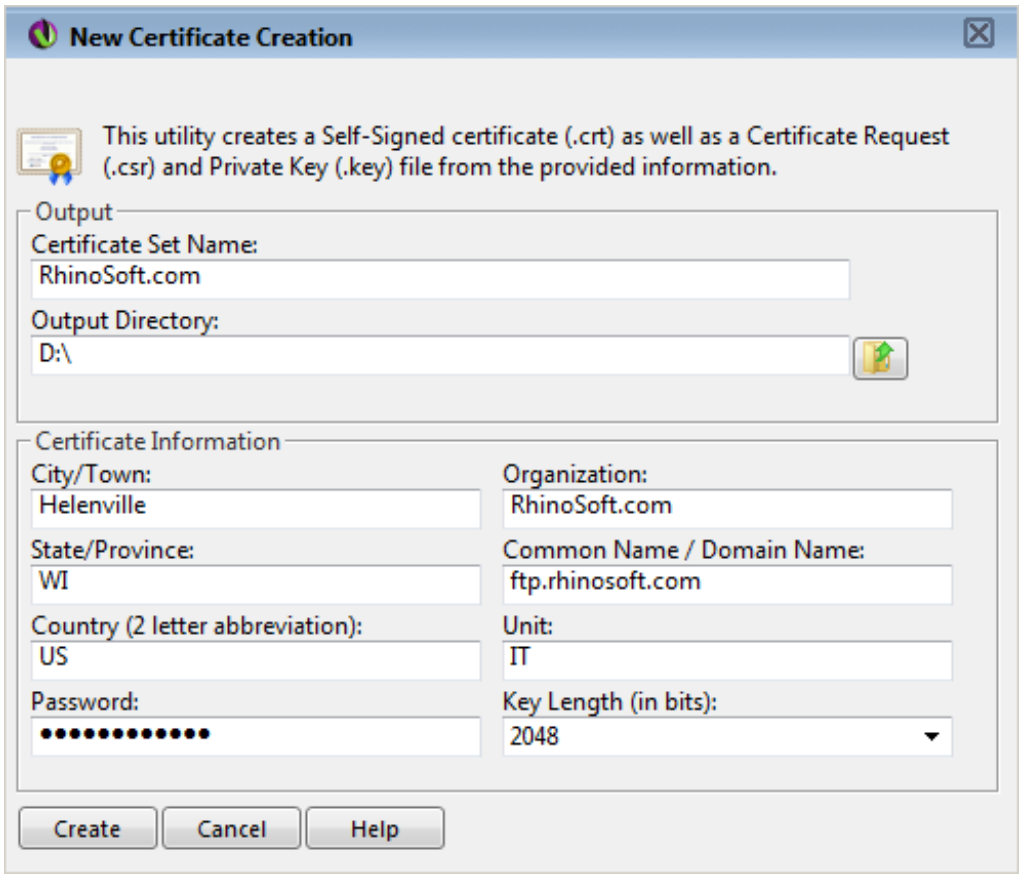
## Using An Existing Certificate

- Obtain an SSL certificate and private key file from a certificate authority.
- Place these files in a secured directory in the server.
- Use the appropriate Browse button to select both the certificate and private key files.
- If a CA (Certificate Authority) PEM file has been issued, enter or browse to the the file.
- Enter the password used to encrypt the private key file.
- Click the Save button.

If the provided file paths and password are all correct, Serv-U begins using the certificate immediately to secure FTPS and HTTPS connections using the provided certificate. If the password is incorrect or Serv-U cannot find either of the provided files, an error message is displayed that explains the encountered error.

## Creating A New Certificate

- Click the Create Certificate button to get started.
- Specify the Certificate Set Name that is used to name each of the files Serv-U creates.
- Specify the output path where the created files are to be placed. In most cases, the installation directory is a safe location (i.e, C:\Program Files\RhinoSoft.com\Serv-U\).
- Specify the city/town in which the server or corporation is located.
- Specify the state (if applicable) in which the server or corporation is located.
- Specify the 2-digit country code for the country in which the server or corporation is located.
- Specify the password used to secure the private key.
- Specify the full organization name.
- Specify the common name of the certificate. The IP address or the Fully Qualified Domain Name (FQDN) that Users use to connect must be listed here. NOTE: If the Common Name is not the IP address or FQDN used by clients to connect, clients may be prompted that the certificate does not match the domain name they are connecting to.
- Specify the business unit the server resides in.
- Click the Create button to complete certificate creation.




Serv-U creates three files using the provided information: A self-signed certificate (.crt) that can be used immediately on the server but isn't authenticated by any known certificate authority, a certificate request (.csr) that can be provided to a certificate authority for authentication, and a private key file (.key) that is used to secure both certificate files. It is extremely important that the private key be kept in a safe and secure location. If your private key is compromised, then your certificate can be used by malicious individuals.

## Viewing The Certificate

To view the SSL certificate once it is configured, click the View Certificate button. All identifying information about the certificate, including the dates during which the certificate is valid, are displayed in a new dialog.

## Advanced SSL Options

These advanced SSL options can only be configured at the Server level. All Domains inherit this behavior, which cannot be individually overridden.

Enable Low Security Ciphers - Checking this box enables low-security SSL ciphers to be used. Some older or international clients may not support today's best SSL ciphers. Because these ciphers are considered insecure by today's computing standards, Serv-U does not accept these ciphers by default.

Disable SSLv2 Support - There are several different versions of SSL supported by Serv-U. An older version, SSLv2, has documented security weaknesses that make it less secure than SSLv3 and TLS. However, it may be necessary to support SSLv2 for compatibility with exported clients or old client software. Checking this box disables support for the older SSLv2 protocol.

## FIPS Options

Enable FIPS 140-2 mode - FIPS 140-2 is a set of rigorously tested encryption specifications set by the National Institute of Standards and Technology (NIST). Enabling FIPS 140-2 mode limits Serv-U to encryption algorithms certified to be FIPS 140-2 compliant and ensures the highest level of security for encrypted connections.

# SFTP (Secure File Transfer over SSH2)

## Using An Existing Private Key

- Obtain a private key file.
- Place the private key file in a secured directory in the server. Use the Browse button in Serv-U to select the file.
- Enter the password for the private key file.
- Click the Save button.

## Creating A Private Key

- Click the Create Private Key button.
- Enter the name of the private key, (e.g., "MyDomain Key"), which is also used to name the storage file.
- Enter the output path of the certificate, (e.g., C:\Program Files\RhinoSoft.com\Serv-U\).
- Select the Key Type (default of DSA is preferred, but RSA is available).
- Select the Key Length (default of 1024 bits provides best performance, 2048 bits is a good median, while 4096 bits provides best security).
- Enter the password to use for securing the private key file.

## SSH Ciphers and MACs

By default, all supported SSH ciphers and MACs (Message Authentication Codes) are enabled for use by the Server. If your specific security needs dictate that only certain ciphers or MACs can be used, you can individually disable unwanted ciphers and MACs by unchecking the appropriate boxes.

# FTP Settings

The Serv-U File Server allows for the customization of the FTP commands that it accepts as well as its responses to FTP commands received. When configuring these options at the Server level, all Domains inherit these customizations. To customize the FTP behavior for a specific Domain, select the appropriate Domain, open the FTP Settings tab for the Domain, and click the Use Custom Settings button. At any time, the Use Default Settings button can be clicked to have the Domain revert back to the Server's default settings.

Customizing the FTP behavior in this way is not recommended except for those very familiar with the FTP protocol and its standard and extended command set.

## Global Properties

When using custom settings, the Global Properties button becomes available.

### Global FTP Responses

Global FTP responses are responses shared amongst most FTP commands, such as the error message sent when a file isn't found. Customizing a global FTP response ensures that the response is used by all other FTP commands rather than having to customize it for each individual FTP command. FTP command responses can contain special macros that allow real-time data to be inserted in to the response. See the Help section on System Variables for more information.

### Server Welcome Message

The Server welcome message is sent in addition to the standard "220 Welcome Message" that identifies the Server to clients when they first connect. If the Include response code in text of message file box is checked, then the 220 response code begins each line of the specified welcome message. To customize the welcome message, enter the path to a text file in Message File Path input box. Use the Browse button to select a file on the computer. Serv-U opens this file and send its contents to connecting clients.

### Advanced Options

Block "FTP_bounce" attacks and FXP (server-to-server transfers) - Checking this box blocks all server-to-server file transfers involving this Serv-U File Server by only allowing file transfers to the IP address in use by the command channel. For more information on "FTP_bounce" attacks, see CERT advisory CA-97.27.

Include response code on all lines of multi-line responses - The FTP protocol defines two ways in which a multi-line response can be issued by an FTP server. Some older FTP clients have trouble parsing multi-line responses that don't contain the 3-digit response code on each line. Check this box if your clients are using an FTP client experiencing problems with multi-line responses from Serv-U.

Use UTF-8 encoding for all sent and received paths and file names - By default, Serv-U treats all file names and paths as UTF-8 encoded strings. It also sends all file names and paths as UTF-8 encoded strings, such as when sending a directory listing. Unchecking this option prevents Serv-U from UTF-8 encoding these strings. When this option is unchecked, UTF8 is not included in the the FEAT command response to indicate to clients that the server is not using UTF-8 encoding.

# Editing FTP Commands & Responses

To edit FTP Commands, select the FTP command to edit and click the Edit button.

## Information

Under the Information tab, basic information about the command is shown along with a link to more information on our website. Each FTP command can also be disabled by checking the Disable command checkbox. Disabled commands are treated as unrecognized commands when they are received from a client.

## FTP Responses

Under the FTP Responses tab, all possible FTP responses to the command as issued by the Server can be modified by clicking on the Edit button for each response. FTP command responses can contain special macros that allow real-time data to be inserted in to the response. See the Help section on System Variables for more information.

## Message Files

Certain FTP commands allow a message file to be associated with them. The contents of a message file are sent along with the standard FTP response. In addition, a secondary message file path is available as a default option. This allows for message files to be specified using a path relative to the User's home directory for the Message File. If the first message file isn't found, then Serv-U attempts to use the Secondary Message File instead. By specifying an absolute file path in the secondary location, you can ensure that each User receives a message file.

The following is a list of all FTP commands that allow specifying a message file:

- CDUP
- CWD
- QUIT

## Advanced Options

Some FTP commands contain advanced configuration options that offer additional ways to configure the behavior of the command. Where available, the configuration option is described in detail in the Management Console. The following is a list of FTP commands containing advanced configuration options:

- LIST

- MDTM
- NLST

## Case File - Custom FTP Command Response

Users connecting to the server need to know how much quota space is available in a given folder when they have completed a transfer. To do this, edit the response to the STOR command to include a report on available space. By default, the 226 (command successful) response to the STOR command (which stores files on the server) is:

"Transfer complete. $TransferBytes bytes transferred. $TransferKBPerSecond KB/sec."

Modify this to include an extra variable:

"Transfer complete. $TransferBytes bytes transferred. $TransferKBPerSecond KB/sec. Remaining storage space is $QuotaLeft."

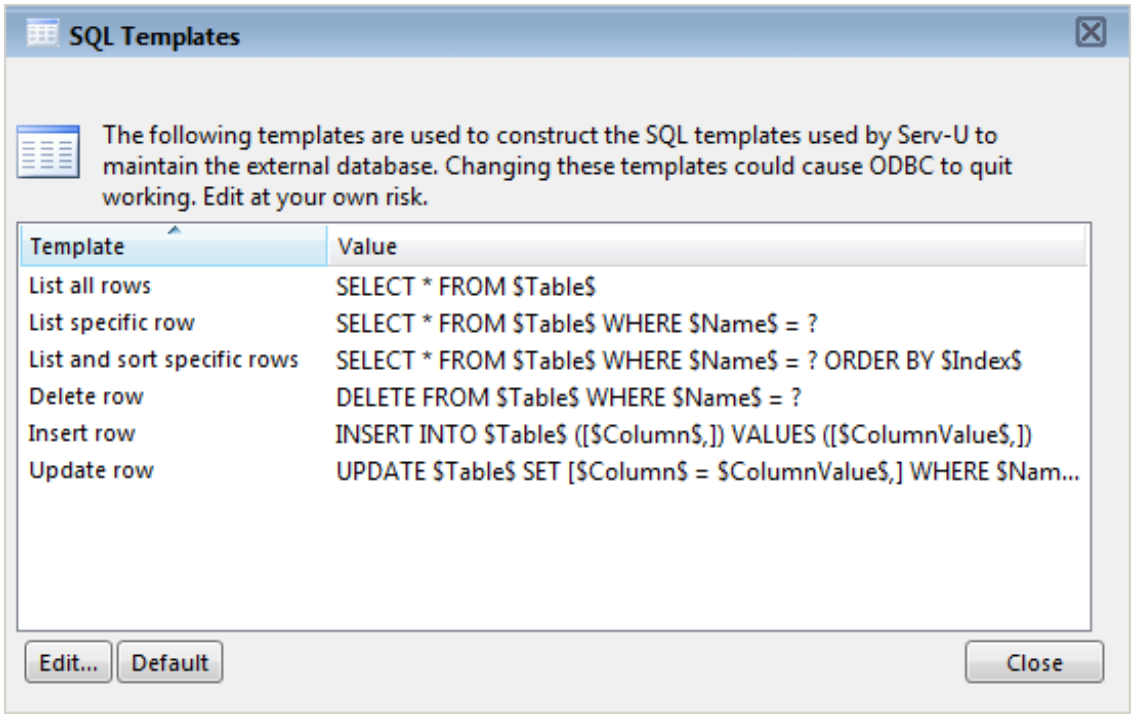
The last sentence shows the user how much storage space is left at the end of each file upload. The same can be done for the DELE command, so that every time a user deletes a file, their updated quota value, showing an increase in available space, is displayed. This can be done for any FTP command response.

# Database Access

## SQL Templates

Serv-U uses multiple queries to maintain the databases containing User and Group information. These queries conform to the SQL language standards. However, if the database you're using is having problems working with Serv-U, you may need to alter these queries. From the SQL Templates dialog, each query used by Serv-U can be specially tailored to conform to the standards supported by your database.

NOTE: Incorrectly editing these SQL queries could cause ODBC support to stop working in Serv-U. Do not edit these queries unless you are comfortable constructing SQL statements and are positive that it is necessary to enable ODBC support with your database software.




## User and Group Table Mappings

By default, Serv-U automatically creates and maintains the tables and columns necessary to store User and Group information in a database. However, if you're attempting to connect Serv-U to an existing database containing this information, you need to customize the table and column names to conform to the existing database structure. Click the User Table Mappings or Group Table Mappings to get started.

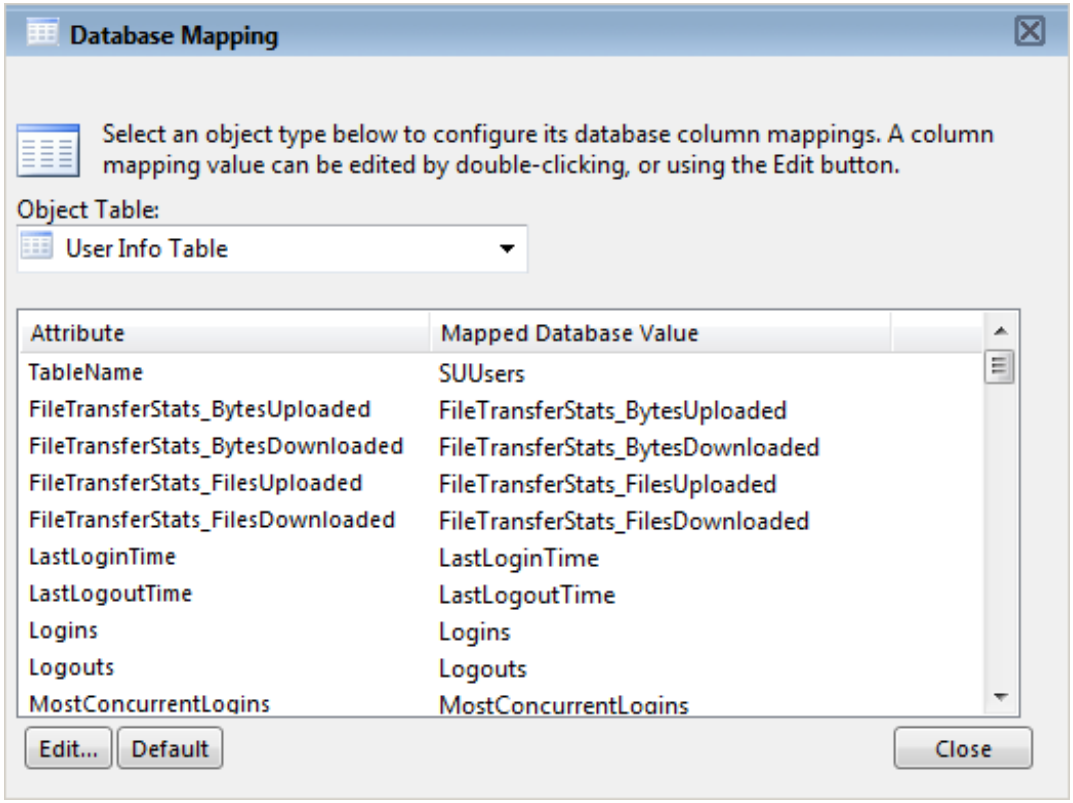
Serv-U stores information for a User or Group in 10 separate tables. Only the User/Group Info Table and User/Group Dir Access Table are required. The current table can be changed from the Object Table drop-down box. The Attribute column lists the attributes that are stored in the current table.

The Mapped Database Value displays the name of the column that attribute is mapped to in the database. The first row always displays the "TableName" and can be used to change the name of the table.

Certain tables where the order of the entries bears significance have a SortColumn attribute listed. This column is used to store the order in which rules are applied.

Click the Edit button or double-click the column name to edit a value.

When enabled, the table is accessed as needed. In special situations a table that isn't being used may be disabled to reduce the number of ODBC (database) calls. For example, if not using Ratios and Quotas "User Ratio-Free Files", "Per User Files Ratio", "Per User Bytes Ratio", "Per Session Files Ratio", and "Per Session Bytes Ratio" tables may be disabled preventing unneeded ODBC calls. Exercise caution when disabling tables as the fields will appear in dialogs, but they will not be saved or loaded. The "User Info" and "Group Info" tables cannot be disabled.




## Case File - ODBC Authentication

Authentication in the Serv-U File Server can be handled through an ODBC database, allowing for scripted account management and maintenance. In order to make use of ODBC functionality, migrate to ODBC authentication through a database. By storing credentials in settings in a database, accounts can be managed from outside the Serv-U Management Console via scripted database operations which can be built into many existing account provisioning systems. A DSN must first be created in Control Panel | Administrative Tools | Data Sources (ODBC) - use a System DSN if Serv-U

is running as a service or a User DSN if Serv-U is running as an application. Once the proper DSN has been created, specify the Data Source Name, login ID and password and select Save. Serv-U creates the tables and columns transparently. Database Users and Groups can be managed from the Database Users and Database Groups sections of Serv-U (located near the normal Users and Groups tabs).

# SMTP Configuration

Serv-U allows administrators to configure an SMTP connection to send email for events configured to use email actions. SMTP can be configured on the server and/or the domain level. SMTP configuration at the domain level may be inherited from the server level. The SMTP configuration dialog is located in the "Events" tab in the "Domain Details" and "Server Details" pages. Simply click on the "Configure SMTP" button to launch the dialog.

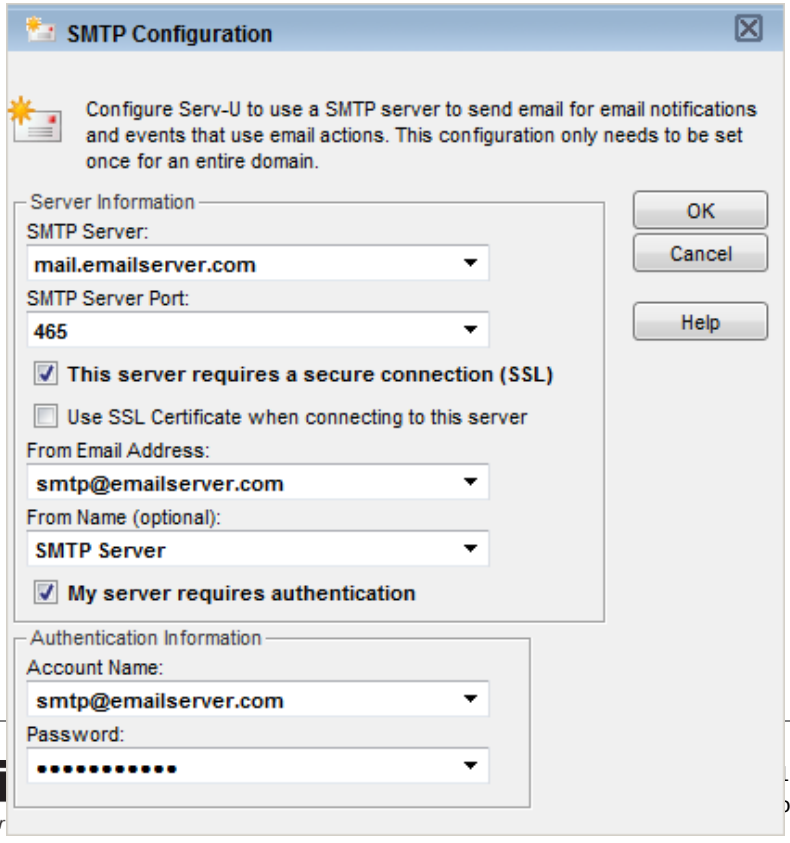
## SMTP Server Information

- SMTP Server - the name or IP address of the SMTP server
- SMTP Server Port - the port the SMTP server is using
- From Email Address - the email address to use for the outgoing email
- From Name (optional) - the name to use for the outgoing email
- My server requires authentication - to enable authentication check this box
- This server requires a secure connection (SSL) - Some SMTP servers require that all incoming connections be encrypted to protect against possible attacks. If your server requires incoming SMTP connections to be encrypted, enable this option. The default port for encrypted SMTP connections is 465. Serv-U supports Implicit SSL only, and does not support Explicit SSL (port 587)

## Authentication Information

If your SMTP server requires authentication you must enter the following information:

- Account Name - the account name associated with authentication for the SMTP server.
- Password - the password for the account.



# Serv-U Events

Serv-U enables the use of event handling which can perform various actions triggered by a list of selected events. Below is a list of actions available to administrators:

## Server Events

- Server Start
- Server Stop

## Server and Domain Events

- Domain Start
- Domain Stop
- Session Connection
- Session Disconnect
- Session Connection Failure
- Log File Deleted

## Server, Domain, User, and Group Events

- User Login
- User Logout
- User Login Failure
- User Password Change
- User Password Change Failure
- User Enabled
- User Disabled
- User Deleted
- IP Blocked
- IP Blocked Time
- Too Many Sessions
- Too Many Session On IP
- IP Auto Added to Access Rules
- User Added
- Password Recovery Sent
- Password Recovery Failed
- File Uploaded
- File Upload Failed
- File Download
- File Download Failed
- File Deleted
- File Moved
- Directory Created
- Directory Deleted
- Directory Changed
- Directory Moved
- Over Quota

- Over Disk Space

## Creating Common Events

Serv-U allows administrators to automatically create a list of the most common events. You may choose to create these common events using email and/or balloon tip actions. Simply click the "Create Common Events" button located in the "Events" tab. Select either the "Send Email" or "Show balloon tip" radio button for the action you want to be performed on the common events. If you choose to "Send Email" you must also enter an "To:" address where the events are to be sent.

# Event Actions

Administrators can select from three different actions that will be executed when an event is triggered. Below is a list of these actions:

- Send Email
- Show Balloon Tip (Server administrator only)
- Execute Command (Server administrator only)

## Email Actions

Email actions can be configured to send emails to multiple recipients and to Serv-U Groups when an event is triggered. To add an email address, enter it in the "To" or "Bcc" fields. To send mail to a Serv-U Group, use the "Group" icon to add or remove Serv-U Groups from the distribution list. Email addresses must be separated with commas or semicolons. Email actions contain an "To", "Subject" and "Message" parameter. Special variables may be used to send specific data pertaining to the event. Please refer to the list of these variables located under "System Variables".

## Balloon Tip Actions

Balloon tip actions can be configured to show a balloon tip in the system tray when an event is triggered. Balloon tip actions contain a "Balloon Title" and "Balloon Message" parameter. Special variables may be used to send specific data pertaining to the event. Please refer to the list of these variables located under "System Variables".

## Execute Command Actions

Execute command actions can be configured to execute a command on a file when an event is triggered. Execute command actions contain an "Executable Path", "Command Line Parameters", and "Completion Wait Time" parameter. For the "Completion Wait Time" parameter, you may enter the number of seconds to wait after starting the executable path. Enter a value of 0 for no waiting.

NOTE: any amount of time Serv-U spends waiting delays any processing that Serv-U can perform.

A wait value should only be used to give an external program enough time to perform some operation, such as move a log file before it is deleted (i.e., $LogFilePath for the "Log File Deleted"

event). Special variables may be used to send specific data pertaining to the event. Please refer to the list of these variables located under "System Variables".

# Serv-U Event Filters

Serv-U Event Filters allow administrators to control to a greater degree when a Serv-U event is triggered. By default, Serv-U Events trigger each time the Event occurs. The Event Filter allows events to be triggered only if certain conditions are met. For example, a standard Serv-U Event might trigger an email each time a file is uploaded to the server. However, using an Event Filter, Events can be triggered on a more targeted basis. A "File Uploaded" event can be configured to only send an email when the file name contains the string "important", so an email would be sent when the file "Important Tax Forms.pdf" is uploaded but not when random other files are uploaded to the server. Additionally, a "File Upload Failed" Event could be set to run only when the protocol used is "FTP", not triggering for failed HTTP or SFTP uploads. This is done by controlling the various variables and values related to the Event and evaluating their results when the Event is triggered.

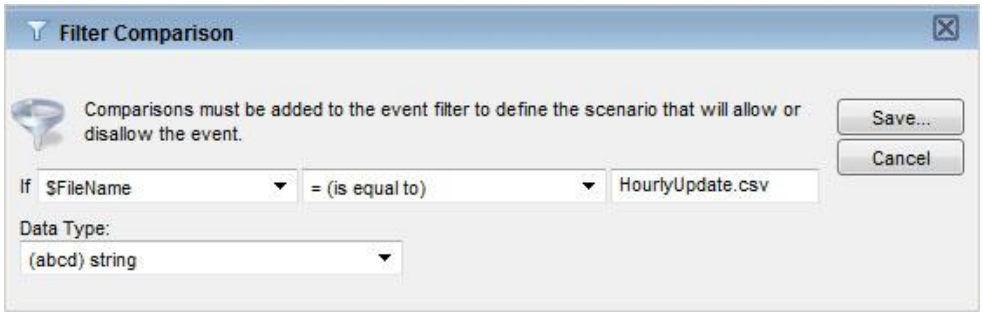
## Event Filter Fields

Each Event Filter has three critical values that must be set:

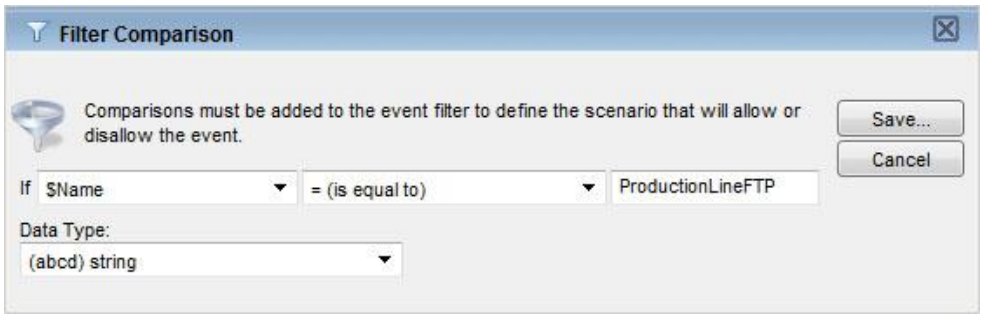
- Name - This is the name of the filter, used to identify the Filter for the Event.
- Description (Optional) - This is the description of the event, which may be included for reference.
- Logic - The "Logic" button determines how the Filter interacts with other Filters for an Event. In most cases, "AND" will be used all filters must be satisfied for the Event to trigger. The function of "AND" is to require that all conditions be met. However, the "OR" operator may be used if there are multiple possible satisfactory responses (for example, abnormal bandwidth usage of less than 20 KB/s OR greater than 2000 KB/s)
- Filter Comparison - This is the most critical portion of the Filter. The Filter Comparison contains the evaluation that must occur for the Event to trigger. For example, a filter can be configured so that only the user "admin" triggers the Event. In this case, the Comparison will be "If $Name = (is equal to) admin", and the data type will be "string". For bandwidth, either an "unsigned integer" or "double precision floating point" value would be used.

## Using Event Filters

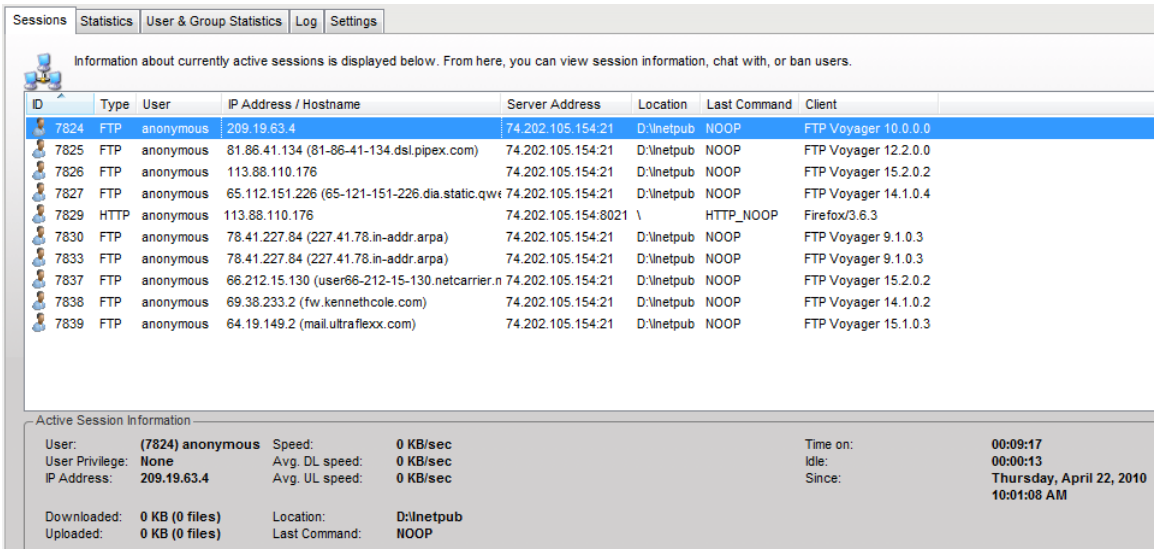
Event filters are utilized by comparing fields to expected values in the Event Filter menu. The best example is firing an Eevnt only when a certain user triggers the action, or when a certain file is uploaded. For example, an administrator may wish to fire an email event when the file "HourlyUpdate.csv" is uploaded to the server, but not other files. To do this, a new Event can be created in the "Domain Details | Events" menu. The Event Type is "File Uploaded", and in the "Event Filter" tab a new filter must be added. The $FileName variable is used and the value is HourlyUpdate.csv as shown below:




As another example, it might be necessary to know when a file transfer fails for a specific user account (perhaps one used by an automated process). To perform this task, create a new "File Upload Failed" event and add a new Filter. The filter comparison will be "$Name", and the value to compare would be the username, such as ProductionLineFTP:



# Tracking Activity In Serv-U




The Server & Domain Session tab displays the current File Server session activity. When viewing the Sessions page from the Server, all connected sessions from all Domains are displayed. When viewed while administering a Domain, only that Domain's current sessions are displayed. From this page, an overall picture of the current activity on the File Server can be seen. In addition, individual sessions can be viewed including their current status, connection state, and transfer information.

To view the detailed information on a specific session, select the session. The Active Session Information group is populated with the details of the currently highlighted session. This information is frequently updated to provide you with an accurate and up-to-date snapshot of that session's activities.

Depending upon the type of connection made by that session, (e.g., FTP, HTTP, or SFTP), certain additional functions are available.

## Disconnect

Any type of session can be disconnected at any time by clicking the Disconnect button. Clicking the button brings up another dialog with additional options for how the disconnect should be performed. There are 3 types of disconnect options available:

- Disconnect - Immediately disconnects the session. Another session can be immediately established by the disconnected client. This is also known as "kicking" the user.
- Disconnect and ban IP - Immediately disconnects the session and bans their IP address for the specified number of minutes, preventing them from immediately reconnecting.
- Disconnect and block IP permanently - Immediately disconnects the session and adds a deny IP access rule for their IP address, preventing them from ever reconnecting from the same IP address.

When disconnecting a session from the Server Session view, an additional option is available called Apply IP rule to. This combo box allows you to select where you would like the temporary or permanent IP ban to be applied - for the entire Server or just the Domain the session is connected to.

In addition to disconnecting the session, the User account in use by the session can also be disabled by checking the box labeled Disable user account.

If the current session is using the FTP protocol, a message can be sent to the user before disconnecting them by typing it in the box labeled Message to user. This option is not available for HTTP or SFTP sessions as neither protocol defines a method for chatting with users.

## Spy & Chat

Any type of session can be spied on by clicking the Spy & Chat button or double-clicking on a session from the list. Spying on a user displays all the detailed information normally visible by highlighting the session, but also includes a complete copy of the session's log since it first connected to the File Server. This allows an administrator to browse the log and view all actions taken by the session's user.

If the current session is using the FTP protocol, additional options are available for chatting with the user. The Chat group shows all messages sent to and received from the session since beginning to "spy" on the session. To send a message to the session, enter the message text in the box labeled Message Content and click the Send button. When a message is received from the session, it is automatically displayed here.

NOTE: Not all FTP clients support chatting with system administrators. The command used to send a message to the server is SITE MSG. In order for a client to receive messages, the client application must be capable of receiving unsolicited responses from the server (instead of just discarding them).

## Broadcast

A message can be sent to all currently connected FTP sessions by clicking the Broadcast button. Sending a message via broadcast is equivalent to opening the Spy & Chat dialog to each individual FTP session and sending it a chat message.

## Abort

If a session is performing a file transfer, the file transfer can be terminated without disconnecting the session by clicking the Abort button. After confirming the abort command, the current file transfer for that session is terminated by the Server. Some clients, especially FTP and SFTP clients, may automatically restart the aborted transfer making it appear that the abort failed. If this is the case, try Disconnecting the session instead.

# Server & Domain Statistics

The Server & Domain Statistics pages show detailed statistics on the use of the Server for use in benchmarking and records keeping. Statistics viewed at the Server level are an aggregate of those accumulated by all Domains on the Server. Statistics viewed for an individual Domain are for that Domain only. The displayed information includes:

## Session Statistics

### Current Sessions

The number of sessions currently connected

### 24 Hrs Sessions

The number of sessions that have connected in the past 24 hours

### Total Sessions

The total number of sessions that have connected since being placed online

### Highest Num Sessions

The highest number of concurrent sessions that has been recorded since being placed online

### Average Session Length

The average length of time a session has remained connected.

### Longest Session

The longest recorded time for a session.

## Login Statistics

These statistics can apply to either a domain or the entire server depending on the statistics currently being viewed. Login statistics differ from session statistics because they apply to a login (providing a login ID and password) as opposed to connecting and disconnection.

### Logins

The total number of successful logins

### Logouts

The total number of logouts

**Currently Logged In**

The number of sessions currently logged in

**Most Concurrent Logins**

The highest number of simultaneously logged in sessions

**Last Login Time**

The last recorded valid login time (not the last time a connection was made)

**Last Logout Time**

The last recorded valid logout time

**Average Duration Logged In**

The average login time for all sessions

Longest Duration Logged In

The longest amount of time a session was logged in

**Shortest Login Duration Seconds**

The shortest amount of time a session was logged in

## Transfer Statistics

**Download Speed**

Cumulative download bandwidth being currently being used

**Upload Speed**

Cumulative upload bandwidth being currently being used

**Average Download Speed**

The average download bandwidth used since being placed online

**Average Upload Speed**

The average upload bandwidth used since being placed online

**Downloaded**

The total amount of data, and number of files, downloaded since being placed online

**Uploaded**

The total amount of data, and number of files, uploaded since being placed online

# User & Group Statistics

The User & Group Statistics pages show detailed statistics based on individual user or group activity. Statistics viewed for a user or group are for that user or group only. The displayed information includes:

## Session Statistics

### Current Sessions

The number of sessions currently connected

### 24 Hrs Sessions

The number of sessions that have connected in the past 24 hours

### Total Sessions

The total number of sessions that have connected since being placed online

### Highest Num Sessions

The highest number of concurrent sessions that has been recorded since being placed online

### Average Session Length

The average length of time a session has remained connected

### Longest Session

The longest recorded time for a session

## Login Statistics

These statistics can apply to either a user or a group of users depending on the statistics currently being viewed. Login statistics differ from session statistics because they apply to a login (providing a login ID and password) as opposed to connecting and disconnection.

### Logins

The total number of successful logins

### Logouts

The total number of logouts

**Currently Logged In**

The number of sessions currently logged in

**Most Concurrent Logins**

The highest number of simultaneously logged in sessions

**Last Login Time**

The last recorded valid login time (not the last time a connection was made)

**Last Logout Time**

The last recorded valid logout time

**Average Duration Logged In**

The average login time for all sessions

**Longest Duration Logged In**

The longest amount of time a session was logged in

**Shortest Login Duration Seconds**

The shortest amount of time a session was logged in

## Transfer Statistics

**Download Speed**

Cumulative download bandwidth being currently being used

**Upload Speed**

Cumulative upload bandwidth being currently being used

**Average Download Speed**

The average download bandwidth used since being placed online

**Average Upload Speed**

The average upload bandwidth used since being placed online

**Downloaded**

The total amount of data, and number of files, downloaded since being placed online

**Uploaded**

The total amount of data, and number of files, uploaded since being placed online

## Save Statistics

User and group statistics can be saved directly to a CSV file for programmatic analysis and review. In order to save statistics to a file, first select the User or Group you wish to generate a statistics file for and then click the "Save Statistics" button on the bottom of the page.

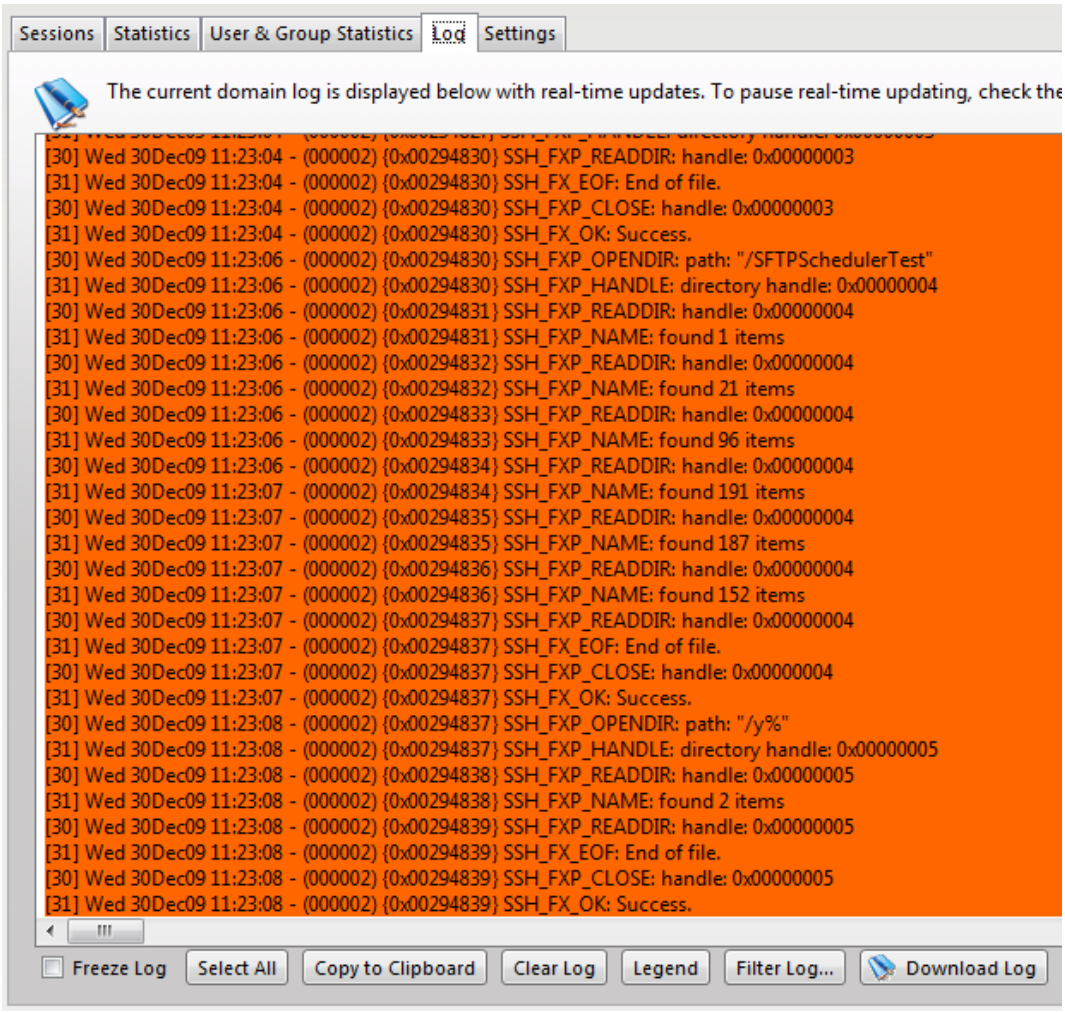
# Server & Domain Log

The Server & Domain Log tab shows logged activity for the Server or Domain.

The Server Log shows File Server start-up, configuration, and shutdown information. It does not show Domain activity information. To activity logs, view the appropriate Domain's log instead. In addition to status information about libraries, licensing, and the current build that is logged when the File Server is first starts, the Server Log also contains information about all Domain listener status, Universal Plug-and-Play (UPnP) status information, and PASV port range status. The information contained in the Server Log is also saved to a text file located in the installation directory that is named Serv-U-StartupLog.txt. This file is replaced each time the Serv-U File Server is started.

The Domain Log contains information about and activity pertaining to the currently administered Domain only. This includes the status of the Domain's listeners and any configured activity log information. For more information on the types of activity information that be placed in the Domain Log, see the Help section entitled Domain Log Settings.

Information contained in the log can be highlighted by clicking and dragging the mouse cursor over the desired portion of the log. Once highlighted, the selected portion can be copied to the clipboard.




## Freeze Log

Check this box to temporarily pause refreshing of the log. This is useful on busy systems so a certain section of the log can be highlighted and copied before it is scrolled out of view. Once finished, uncheck the box to resume automatic updating of the log.

## Select All

Clicking this button automatically freezes the log and highlights all currently displayed log information so that it can be copied to the clipboard.

## Clear Log

When the log has become too large for you to view at once, click this button to erase the currently displayed log information. Only log information received after clicking the button is displayed.

## Legend

To make viewing the different components of the log easier, each different type of logged message is color-coded for quick identification. Clicking this shows the legend in a draggable dialog. Drag the legend dialog to a convenient location so it can be used for reference while browsing the log.

## Filter Log

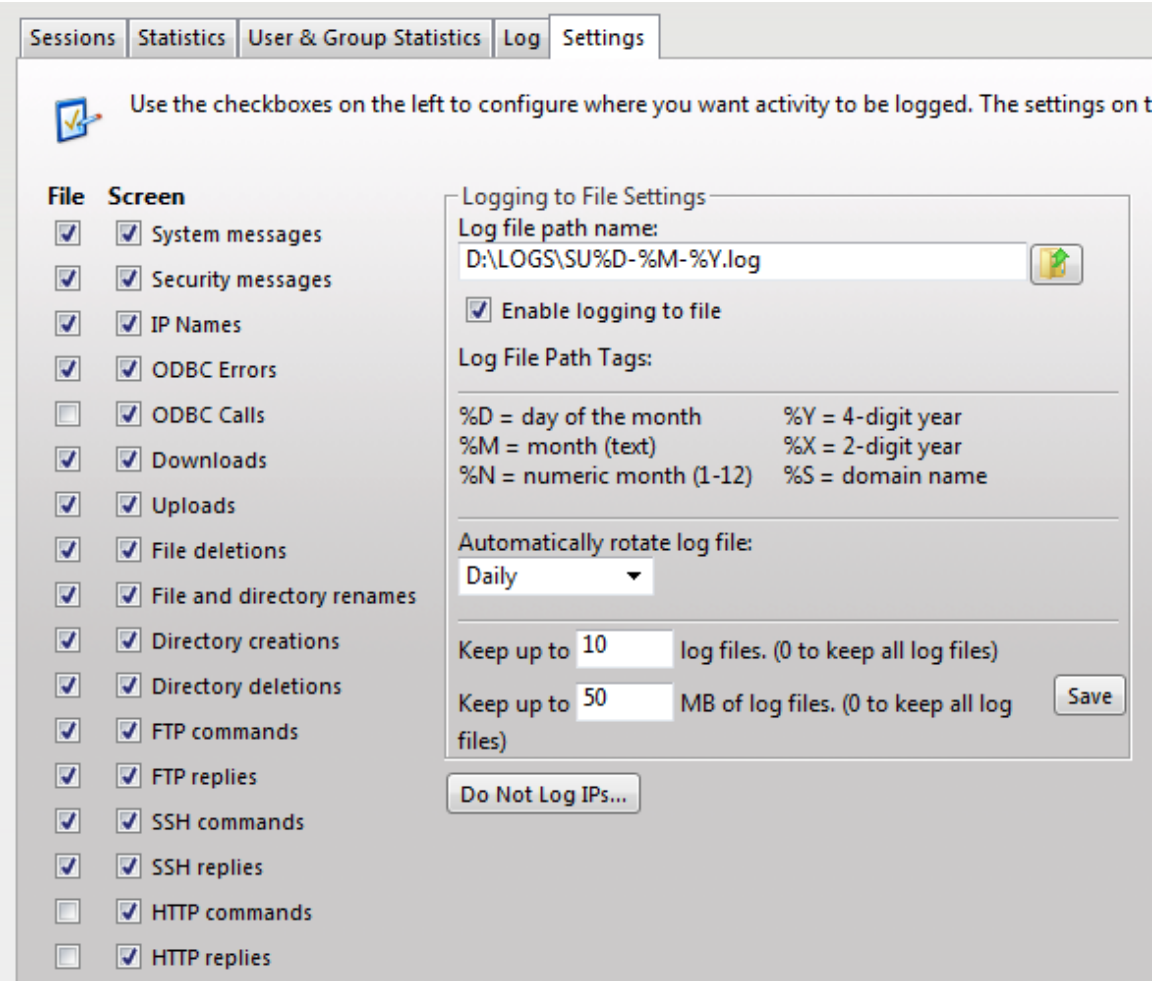
To quickly find and read through specific sections of the log, it can be filtered based upon a search string. Clicking this button brings up the Filter Log dialog. Providing a search string and clicking the Filter button refreshes the log to only display log entries containing the search string. To view the entire contents of the log again, open the Filter Log dialog and click the Reset button.

## Download Log

To download the full log file from Serv-U, click the "Download Log" button. If you have permission to download the file your web browser will prompt you to choose a location to save the file, or begin downloading the file automatically.

# Configuring Domain Logs

The Serv-U File Server allows for a great deal of customization in logging Domain events and activity. Logging is broken into two sections: File and Screen. To enable a logging option, check the appropriate box in the File or Screen column. When an option is checked from the "File" column, the appropriate logging information is saved to the specified log file if Enable logging to file is checked. When an option is checked from the "Screen" column, then the event is displayed in the log when viewed from the Serv-U Management Console. The log can be configured to show as much or as little information as you desire. After configuring the desired logging options, click the Save button to save the changes.




## Logging to File Settings

### Log file path

The log file must be given a name before information can be saved to a file. The Browse button can be used to select an existing file or directory location for the log file. The log file path supports certain

wildcard characters as outlined below. Wildcard characters referencing the date applies to the day that the log file is created. When combined with the Automatically rotate log file option, wildcards provide an automatic way to archive Domain activity for audits, such as those required by HIPAA. The available wildcard characters are:

- %D - The current day of the month
- %M - The name of the current month
- %N - The numeric value of the current month (1-12)
- %Y - The 4-digit value of the current year, (e.g., 2009)
- %X - The 2-digit value of the current year, (e.g., 09 for 2009)
- %S - The name of the Domain whose activity is being logged

## Enable logging to file

Check this box to Serv-U to begin saving log information to the file specified in the Log file path. If this option is not checked, Serv-U does not log any information to the file, regardless of the individual options checked in the "File" column.

## Automatically rotate log file

To ensure that log files remain a manageable size and can be easily referenced during auditing, Serv-U supports the ability to automatically rotate the log file on a regular basis. By specifying a Log file path containing wildcards referencing the current date, Serv-U can rotate the log file and create a unique file name every day, week, month, or year.

## Purge Old Log Files

Serv-U supports the ability to automatically purge old log files by setting a maximum number of files to keep and/or a maximum size limit in MB's. Setting these options to "0" means the setting is unlimited and the limit is not applied.

CAUTION: Log files are purged based only on the current log file path name. Log file variables are replaced with Windows wildcard values used to search for matching files. For example:

C:\Logs\%Y:%N:%D %S Log.txt is searched for C:\Logs\????:??:?? * Log.txt
C:\Logs\%Y:%M:%D %S Log.txt is searched for C:\Logs\????:*:?? * Log.txt
C:\Logs\%S\%Y:%M:%D Log.txt is searched for C:\Logs\--DomainName--\????:*:?? Log.txt

Log variables are wildcarded like this:

%D --> ??
%N --> ??
%M --> *
%Y --> ????
%X --> ??
%S --> *

Anything matching the wildcarded path name can be purged. Use caution; it's best practice to place log files into a single directory to avoid unexpected file deletion.

## Do Not Log IPs

Serv-U supports the ability to specify IP addresses that are exempt from logging. Activity from these IP addresses is not logged to the location specified by the rule - the Screen, a File, or both. This is useful to exempt IP addresses for administrators that may otherwise generate a lot of logging information that can obfuscate Domain activity from regular users. It can also be used to save on log space and reduce overhead. Simply click the Do Not Log IPs button and add IP addresses as appropriate.

# Database Support

Serv-U enables the use of an ODBC database to store and maintain group and user accounts at both the Domain and Server levels. The ODBC connections are configured from two locations: Domain | Domain Details | Database and Server | Server Details | Database. Serv-U can automatically create all of the tables and columns necessary to begin storing Users and Groups in your database. Because Serv-U uses one set of table names to store its information, individual ODBC connections must be configured for each item which stores details in the database. In other words, the Server as well as each Domain must have a unique ODBC connection to ensure they are stored separately. To configure a database, follow these steps:

- Create an ODBC connection for Serv-U to use. RhinoSoft.com recommends MySQL, but any database that has a Windows ODBC driver available can be utilized. Use a System DSN if Serv-U is operating as a system service, or a User DSN if Serv-U is operating as a regular application.
- Open the Serv-U Management Console and browse to the appropriate Domain or Server database settings. Enter the Data Source Name (DSN), the login ID, and Password and click Save.

If the database connection is being configured for the first time, leave the Automatically create options checked. With these options checked, the Serv-U File Server builds the database tables and columns automatically.

# License Information

The License Details tab displays the information contained in the current registration ID in use by the Serv-U File Server. If the installation is running in trial mode, then information on the number of trial days remaining is also included. Information contained on this tab includes:

## Name

The name associated with the current license

## Email Address

The email address associated with the current license

## Serv-U Edition

The Serv-U Edition that is enabled by the current license. See Serv-U Editions for more information

## Copies

The number of concurrent installations allowed by the current license

## Purchase Date

The date the current license was purchased.

## Updates

The date through which the current license allows free updates to the latest version. If running as a trial, the number of trial days remaining is displayed

## Edition Information

Displays enabled functionality and limitations of the licensed Serv-U Edition

## Additional Products

Additional add-ons for Serv-U and whether or not they are enabled

# Registering Serv-U

To Register the Serv-U File Server, click the Register button on the bottom toolbar and enter your alphanumeric registration ID. If you have lost your ID, click on the Lost ID button for assistance in

retrieving it. If you need to purchase an ID, click on the Purchase button to visit our web site to purchase an ID.

# System Variables

Certain configurable messages in Serv-U can be customized to include a wide range of variables as outlined in the list below. These variables are replaced at run-time with the appropriate value allowing up-to-date statistics and feedback to be provided to logged in Users. Some of the places where these variables can be used include in Event messages, a customized FTP command response, or a Welcome Message.

All available variables and a short explanation of each is included below. Statistical information, unless otherwise specified, is calculated since the Serv-U File Server was last started.

## Server Information

- $ServerName - The full name of the server, (i.e., Serv-U)
- $ServerVersionShort - The first two digits of the current version of the Serv-U File Server, (e.g., 7.0)
- $ServerVersionLong - The full version number of the Serv-U File Server, (e.g., 7.0.0.3)
- $OS - The name of the operating system, (e.g., Windows XP)
- $OSVer - The full version number of the operating system, (e.g., 5.1.2600)
- $OSAndPlatform - The name of the operating system, (e.g., Windows XP) and platform (e.g., 32-bit or 64-bit)
- $ComputerName - The name of the computer retrieved from the operating system, normally the same as the UNC name on a Windows network (e.g., WEB-SERVER-01)
- $LogFilePath - Retrieves the path to the log file (Log File Deleted Event only)

## Server Statistics

- $ServerDays - The total number of days the Server has been online continuously
- $ServerHours - The number of hours from 0 to 24 the Server has been online, carries over to $ServerDays
- $ServerMins - The number of minutes from 0 to 60 the Server has been online, carries over to $ServerHours
- $ServerSecs - The number of seconds from 0 to 60 the Server has been online, carries over to $ServerMins
- $ServerKBup - The total number of kilobytes uploaded
- $ServerKBdown - The total number of kilobytes downloaded
- $ServerFilesUp - The total number of files uploaded
- $ServerFilesDown - The total number of files downloaded
- $ServerFilesTot - The total number of files transferred, essentially ($ServerFilesUp + $ServerFilesDown)
- $LoggedInAll - The total number of established sessions
- $ServerUploadAvgKBps - The average upload rate in KB/s
- $ServerDownloadAvgKBps - The average download rate in KB/s
- $ServerAvg - The average data transfer rate (uploads and downloads) in KB/s
- $ServerUploadKBps - The current upload transfer rate in KB/s
- $ServerDownloadKBps - The current download transfer rate in KB/s
- $ServerKBps - The current aggregate data transfer rate in KB/s

- $ServerSessions24HPlusOne - The total number of sessions in the past 24 hours plus one additional session
- $ServerSessions24H - The total number of sessions in the past 24 hours

## Domain Statistics

- $DomainKBup - The total number of kilobytes uploaded
- $DomainKBdown - The total number of kilobytes downloaded
- $DomainFilesUp - The total number of files uploaded
- $DomainFilesDown - The total number of files downloaded
- $DomainFilesTot - The total number of files transferred, essentially ($DomainFilesUp + $DomainFilesDown)
- $DomainLoggedIn - The total number of sessions currently connected
- $DomainUploadAvgKBps - The average upload rate in KB/s
- $DomainDownloadAvgKBps - The average download rate in KB/s
- $DomainAvg - The average aggregate data transfer rate (uploads and downloads) in KB/s
- $DomainUploadKBps - The current upload transfer rate in KB/s
- $DomainDownloadKBps - The current download transfer rate in KB/s
- $DomainKBps - The current aggregate data transfer rate in KB/s
- $DomainSessions24HPlusOne - The total number of sessions in the past 24 hours plus one additional session
- $DomainSessions24H - The total number of sessions in the past 24 hours

## User Statistics

Applies to all sessions attached to the User account

- $UserKBUp - The total number of kilobytes uploaded
- $UserKBDown - The total number of kilobytes downloaded
- $UserKBTot - The total amount of kilobytes transferred
- $UserLoggedIn - The total number of sessions
- $UserUploadAvgKBps - The average upload rate in KB/s
- $UserDownloadAvgKBps - The average download rate in KB/s
- $UserAvg - The average aggregate data transfer rate (uploads and downloads) in KB/s
- $UserUploadKBps - The current upload transfer rate in KB/s
- $UserDownloadKBps - The current download transfer rate in KB/s
- $UserKBps - The current aggregate data transfer rate in KB/s
- $UserSessions24HPlusOne - The total number of sessions in the past 24 hours plus one additional session
- $UserSessions24H - The total number of sessions in the past 24 hours

## Last Transfer Statistics

Applies to the most recently completed successful data transfer

- $TransferBytesPerSecond - The effective (compressed) transfer rate in bytes/s
- $TransferKBPerSecond - The effective (compressed) transfer rate in KB/s
- $TransferBytes - The effective (compressed) number of bytes transfered, formatted for display, e.g., 32,164
- $NoFormatTransferBytes - The effective (compressed) number of bytes transfered, unformatted, e.g., 32164

- $TransferKB - The effective (compressed) number of kilobytes transfered, formatted for display
- $ActualTransferBytesPerSecond - The actual (uncompressed) transfer rate in bytes/s
- $ActualTransferKBPerSecond - The actual (uncompressed) transfer rate in KB/s
- $ActualTransferBytes - The actual (uncompressed) number of bytes transfered, formatted for display, e.g., 32,164
- $NoFormatActualTransferBytes - The actual (uncompressed) number of bytes transfered, unformatted, e.g., 32164
- $ActualTransferKB - The actual (uncompressed) number of kilobytes transfered, formatted for display
- $CompressionRatio - The ratio of compression for the transfer expressed as a percentage of the expected amount of data transfered. For example, a value of 100.00 means the data could not be compressed. A value of 200.00 means the data compressed to half its original size.
- $CurrentCompressedTransferBytes - The current effective (compressed) number of bytes transfered so far, unformatted, e.g., 32164 (FTP only)
- $CurrentUncompressedTransferBytes - The current actual (uncompressed) number of bytes transfered so far, unformatted, e.g., 32164 (FTP only)

## Date/Time

- $Date - The current date according to the Serv-U File Server, in the system's local date format
- $Time - The current time according to the Serv-U File Server, in the system's local time format

## Server Settings

- $MaxUsers - The maximum number of sessions allowed to login, which could be limited by the license
- $MaxAnonymous - The maximum number of anonymous users allowed to login

## Session Information

Applies to the current session

- $Name - The login ID of the attached User account
- $LoginID – The session's login ID, operates like $Name. $Name can refer to the login ID for target user accounts but $LoginID refers only to the login ID of the session.
- $IP - The client IP address
- $IPName - The reverse DNS name as obtained by performing a reverse DNS lookup on $IP
- $Dir - The session's current directory
- $Disk - The local drive letter being accessed
- $DFree - The amount of free space on $Disk in MB
- $FUp - The total number of files uploaded
- $FDown - The total number of files downloaded
- $FTot - The total number of files transferred, essentially ($FUp + $FDown)
- $BUp - The total number of kilobytes uploaded
- $Bdown - The total number of kilobytes downloaded
- $BTot - The total number of kilobytes transferred
- $TConM - The total number of minutes the session has been connected

- $TConS - The number of seconds from 0 to 60 that the session has been connected, carries over to $TconM
- $RatioUp - The 'upload' portion of the applied ratio, "N/A" if not in use
- $RatioDown - The 'download' portion of the applied ratio, "N/A" if not in use
- $RatioType - The type of ratio being applied, either per session or per User
- $RatioCreditType - The type of ratio credit granted for transfers, either per bytes or per complete file
- $RatioCredit - The current transfer credit for the applied ratio, either megabytes or complete files
- $QuotaUsed - Displays how much disk quota is currently being used in MB, "Unlimited" if no quota is in use
- $QuotaLeft - Displays how much disk quota is available in MB, "Unlimited" if no quota is in use
- $QuotaMax - Displays the maximum amount of disk space that can be used in MB, "Unlimited" if no quota is in use
- $Protocol - The current protocol being used (FTP, FTPS, HTTP, HTTPS, or SFTP (SSH2))
- $DomainName - The current domain that the session is logged into
- $DomainDescription - The description of the current domain that the session is logged into
- $TimeRemaining - The time remaining when blocking an IP address for an amount of time (available only in Event notifications)
- $LocalHomeDirectory - The local home directory. It should only be used for events that need this specific information such as user creation.
- $Password - The password associated with the user account. It is intended only for events. It should NOT be used for welcome messages.
- $UserEmailAddress - The user's email address.
- $FullName - The user's full name as entered into the "Full Name" field for a user account.
- $SpaceFullName - The same as "$FullName" with the addition of a space before the user's full name. Blank (no space or name) when the user's full name is empty.
- $FullNameSpace - The same as "$FullName" with the addition of a space after the user's full name. Blank (no space or name) when the user's full name is empty.

NOTE: Using the $IPName variable inside of an event or sign-on message can cause a slight delay while the reverse DNS information for $IP is retrieved.

## File Information

Applies to the last remotely accessed file, which is not necessarily the last transferred file

- $PathName - Retrieves the full remote path
- $FileName - Retrieves just the filename from $PathName
- $FileSize - Retrieves the size, in bytes, of the file from $FileName
- $FileSizeFmt - A formatted version of the file size, containing the thousands separator (comma or period depending on the computer's regional settings)
- $FileSizeKB - A formatted floating point value representing the file size in KB
- $LocalPathName - Retrieves the fully qualified local path name for an operation, as it relates to Windows. For example "C:\Temp\File.fid" instead of "/Temp/file.fid"
- $LocalFileName - Retrieves the name of the file as it is stored on the local computer. See $LocalPathName for details
- $OldLocalPathName - Same as $LocalPathName, but contains the path prior to renaming
- $OldLocalFileName - Same as $LocalFileName, but contains the file name prior to renaming
- $OldPathName - Retrieves the remote path name prior to renaming

- $OldFileName - Retrieves the remote file name prior to renaming

## Current Activity

- $UNow - The current number of sessions on the Serv-U File Server
- $UAll - The total number of sessions that have connected to the Serv-U File Server since it was last started
- $U24h - The total number of sessions that have connected to the Serv-U File Server in the last 24 hours
- $UAnonAll - The current number of sessions attributed to the anonymous user on the Serv-U File Server
- $UAnonThisDomain - The current number of sessions attributed to the anonymous user on the connected Domain
- $UNonAnonAll - The current number of sessions not attributed to the anonymous user on the Serv-U File Server
- $UNonAnonThisDomain - The current number of sessions not attributed to the anonymous user on the connected Domain
- $UThisName - The current number of sessions attributed to the connected User account

# Web Client Parameters

The Serv-U Web Client supports several parameters that can enhance log on in various ways. Special login links can be created in the Web Client that allow users to automatically send their Login ID and password, start audio files immediately, start in Thumbnail Mode and more. To specify these parameters, add a forward slash after the URL of the server, a "?" character and then these parameters with an ampersand "&" between them. The parameters supported in the Serv-U Web Client are:

- user=*username*&password=*password* – Allows the Login ID and password to be sent automatically to Serv-U, bypassing the need to log in. This can be very convenient for audio/video but should NOT be used for confidential or protected information.
- thumbnail=1 – Starts the Web Client in Thumbnail Mode, showing thumbnails of all images.
- slideshow=1 – Starts the Web Client in Slideshow Mode, showing a slideshow of all images.
- playlist=1 – Starts the Web Client in media mode, playing audio/video files in order.
- playmedia=1 – Starts the web client in media mode, playing a video files only.
- dir=*directory* – Specifies what directory to browse into immediately after login.
- file=*file* – Specifies a file to download immediately after login, defaulting in the home directory. If the "dir" command is used in conjunction with "file", the Web Client attempts to download a file from that folder.
- sortcol=*column* – Specifies the column by which to sort the files in the Web Client. This column accepts the integer values 1-3 for sorting by name, size, or time.

Some examples follow:

**http://yourserver.com/?user=admin&password=test&file=weeklyreport.csv** - This link will log in the user "admin" and automatically download the file called "weeklyreport.csv" if it exists.

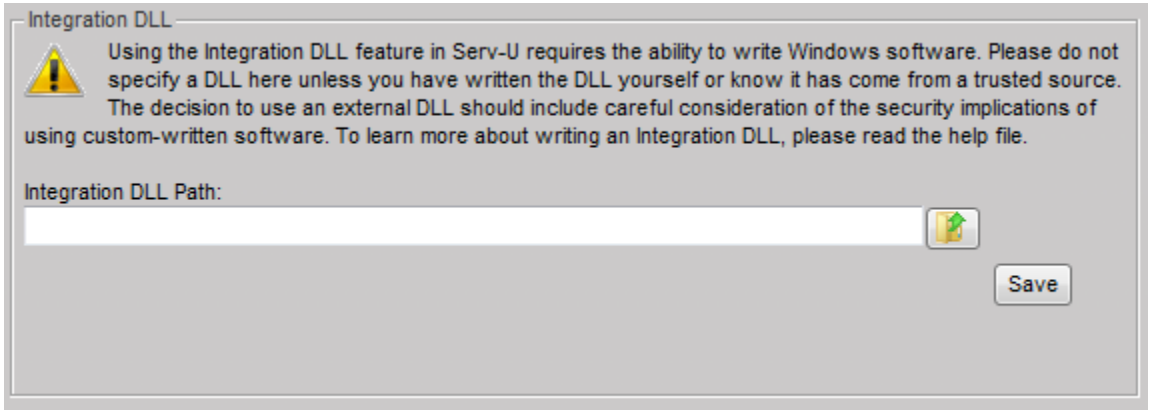
- **http://yourserver.com/?user=presentations&password=ads&dir=/onsite/&playmedia=1** – This link will log in the user "presentations" and play the video files found in the "onsite" directory in order, perhaps for an on-site presentation of a product.
- **http://yourserver.com/?user=dj&password=music&sortcol=3&playlist=1** – This link will log in the user "dj" and automatically begin playing audio files in order of last modification date.
- **http://yourserver.com/?user=familyreunion&password=reunion&slideshow=1** – This link will log in the user "familyreunion" and automatically start playing a slideshow of images, a link that might be shared with family members after an event.

# Serv-U Integration DLL

The Serv-U File Server includes a fully-extensible Integration DLL which allows nearly every function of Serv-U from user login, authentication, password changes, and more to be delgated to external code via an easy-to-build DLL. The DLL is fully documented via code found in the "Serv-U Integration Sample DLL" folder in the Serv-U installation directory.

## Configuring the Integration DLL

The Integration DLL can be configured for both the Domain and Server levels. If an Integration DLL is defined for the Server level, it will also be used for all Domains that do not already have an Integration DLL defined. Integration DLLs configured at the Domain level will override those configured at the Server level. The Integration DLL is configured in the "Limits and Settings | Settings" menu at etiher the Domain or Server level.




**NOTE:** Because Serv-U is available in both 32-bit and 64-bit builds, an extra level of complexity must be considered when building your Integration DLL. If you are running the 64-bit build of Serv-U, you must also build your DLL as a 64-bit DLL instead of as a 32-bit DLL. If you are running a 64-bit build of Windows and are not sure whether you are using the 64-bit build of Serv-U, you can check in the Windows Task Manager. A 32-bit build of Serv-U will include "*32" next to the executable name, as shown below.

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| Serv-U.exe *32 | thomas | 00 | 18,040 K | -24 K | 8,704 K | 27,366 | 0 | 331 | 21 | Serv-U® ... |
| Serv-U-Tray.exe *32 | thomas | 00 | 51,260 K | 0 K | 26,764 K | 68,234 | 20 | 496 | 21 | Serv-U® ... |

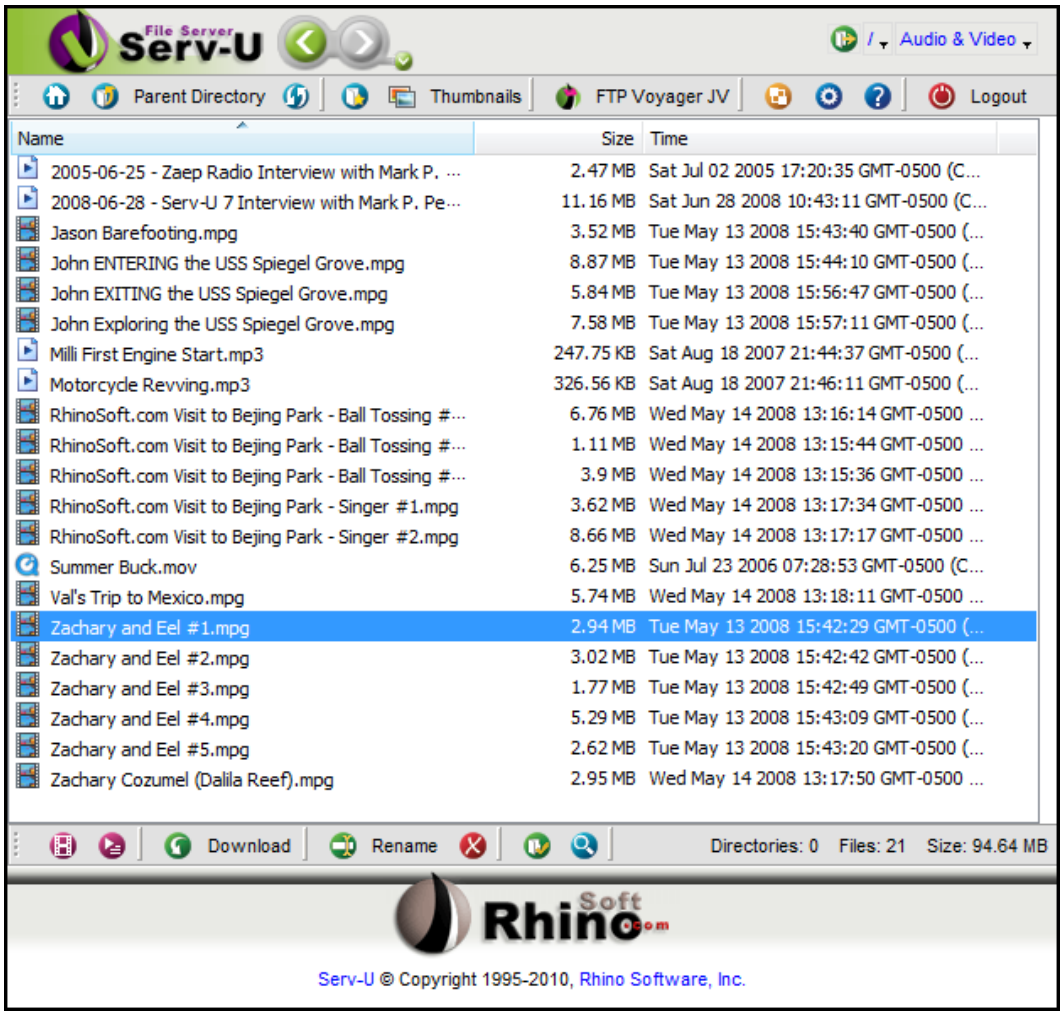
# Built-In Clients

The Serv-U File Server includes two built-in file transfer clients that can be utilized without installing any software or utilities on computers used to access files through Serv-U. Each license of Serv-U includes the Web Client, an advanced web-based file transfer client that operates as a web site and is accessible from any browser. Also available is the advanced FTP Voyager JV client, a Java application accessible using the browser that extends further function to users with minimal overhead and configuration required.

## Serv-U Web Client

The Serv-U Web Client is an advanced web-based file transfer client that allows users to perform any file transfer work via any well-supported browser. Serv-U supports Mozilla Firefox, Internet Explorer, Apple Safari, Google Chrome, and Opera. From the Web Client, users can upload, download, rename, and delete files.

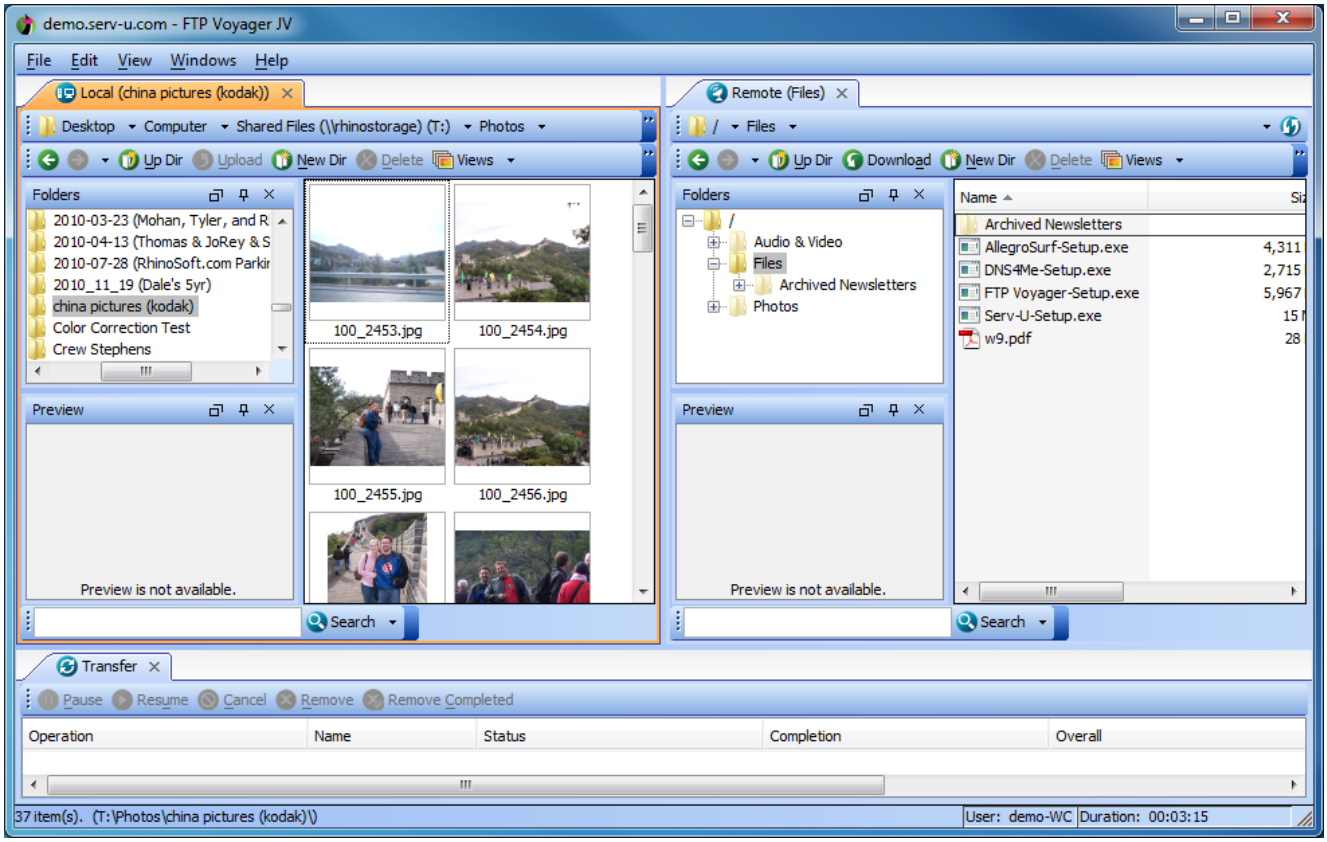
In addition, the Web Client has extensive function as a media server. Using the Web Client, users can stream audio and video files as well as view image previews and even slide shows. With advanced Web 2.0 foundations, the Web Client can provide files to users using a nimble and easy-to-use site.




# FTP Voyager JV

FTP Voyager JV is the most powerful file transfer client available in the Managed File Transfer sphere. As a highly advanced Java file transfer application, FTP Voyager JV allows users to connect to Serv-U anytime, anywhere without needing to install software. This goes a step beyond the Web Client, adding features that break free of browser limitations like full directory synchronization, a customizable tabbed user interface, lockable navigation between tabs, and more. FTP Voyager JV can offer simple drag/drop file transfer functionality or a highly sophisticated experience based solely on the experience and needs of end-users.

As a Java application, FTP Voyager JV runs outside the browser and is portable to clients running Mac OS X, Windows, Linux, and Solaris. Multi-platform functionality becomes even more essential when working in firms where users have different platforms (e.g., a graphics firm where Macs are used by artists while Windows PCs are used by IT and accounting). By delivering file transfer functionality from the server, administrators do not need to install or manage clients-side software – they only need to provide the login link and credentials, and users throughout the organization can do the rest.



# Glossary

- **Server** – The Serv-U File Server, and the main Serv-U engine which handles incoming FTP/FTPS/SFTP/HTTP/HTTPS requests. Settings set at the Server level will be inherited by all Domains, Groups and Users.
- **Domain** – A collection of Users and Groups which use the same Listeners and common settings.
- **Group** – A group of Users who share common settings, such as Virtual Paths or Directory Access rules.
- **User** – A single account which allows a user to log on to Serv-U and access files and folders.
- **Listener** – A listening service in Serv-U which is configured in a Domain to accept incoming FTP, FTPS, SFTP, HTTP or HTTPS connections. Listeners may be either IPv4 or IPv6, but not both.
- **Limit** – A configuration option which can be set at the Server, Domain, Group, or User level. Limits can be set for password complexity requirements, session timeout, Web Client customization and more.
- **FTP** – Acronym for "File Transfer Protocol", one of the first methods of sharing files on the Internet. Still in common use, but more commonly replaced with secure protocols like FTPS, SFTP or HTTPS for security reasons.
- **FTPS** – Acronym for "FTP over SSL", an FTPS connection is identical to an FTP connection except that the FTPS connection is encrypted using SSL. FTPS works by securing usernames, passwords, and files from being stolen or intercepted in transit. FTPS Support is available in Serv-U Silver and Gold Editions.
- **SFTP** – Acronym for Secure File Transfer Protocol, SFTP is actually unrelated to FTP. SFTP is a secure method of transferring files using the SSH protocol, and is essentially a subset of SSH since SFTP can transfer files but cannot open a shell session. SFTP support is available in Serv-U Gold Edition.
- **HTTP** – Acronym for Hypertext Transfer Protocol, HTTP is how most web sites are shared over the Internet. Serv-U includes an HTTP interface for use with the Web Client and FTP Voyager JV. HTTP is available in all three Serv-U Editions.
- **HTTPS** - Acronym for HTTP Secure, HTTPS is a secured method of connecting to a Web Server. HTTPS support is available in Serv-U Gold Edition.
- **Public Key Authentication** – Public Key Authentication, or PKA, is a process in SFTP by which users may authenticate to Serv-U using a key pair instead of a password. This is a very

secure way to connect, and is used frequently by automated cron jobs in Unix-based operating systems.

- **Event** – A Serv-U event consists primarily of an event type (User Login, File Upload Failed, etc) and an Action type (Show Balloon Tip, Send Email, or Execute Command). Serv-U events are used to automate behavior and provide greater visibilty of important file transfer processes.

- **Anti-Hammering** – A Serv-U feature which allows administrtors to block IP addresses who attempt to connect repeatedly with incorrect credentials. By intelligently handling only IP addresses who repeatedly fail to log on correctly, Anti-Hammering allows for smart blocking of bots and hackers.

- **Web Client** – The Serv-U Web Client is a web-based file transfer interface that is provided free of charge in all Serv-U Editions. An advanced Web 2.0 service, the Web Client can be used to upload, download, delete, and rename files just like any other client. It can also be used to drag/drop files, play media, or render slideshows and thumbnails of images.

- **FTP Voyager JV** – FTP Voyager JV is an advanced multi-platform file transfer client available as an add-on for the Serv-U File Server. Based on Java, it is launched through the HTTP/HTTPS interface and allows full drag/drop functionality and integration with the desktop for a seamless transfer experience.

- **AES** – Acronym for Advanced Encryption Standard. AES is a strong encryption standard used by the US Government and many corporations for encrypting data while in transit. AES is available in Serv-U in 128-bit, 192-bit, and 256-bit ciphers.

- **Directory Access** – Encompasses all of the permissions applied to a Server, Domain, Group, and User, which grant and deny permission to files and folders. Directory Access rules are the foundation of file access rights, determining what a user may and may not access (as well as how they may access it).

- **IP Access** – IP Access rules are used in Serv-U to determine who may connect to the server. Rules defined at the Server and Domain levels define who is allowed to make an initial connection to Serv-U, while rules defined at the User and Group levels define who may connect using a given user account.

- **Remote Administration** – Through the HTTP/HTTPS services in Serv-U, Serv-U Gold Edition customers are able to connect to Serv-U remotely to administer services and users without actually logging on to the server itself. This allows for easier administration of remote servers.

- **UPnP** – UPnP stands for Universal Plug and Play, and is a method used by software to automatically configure routers and firewalls for network services. Serv-U includes UPnP support for IPv4 and IPv6 routers.